IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

TEXTILE COMPUTER SYSTEMS, INC., Plaintiff, v. AMARILLO NATIONAL BANK, Defendant.	CIVIL ACTION NO. 6:22-cv-932 ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Textile Computer Systems, Inc. ("Textile" or "Plaintiff") files this original complaint against Defendant Amarillo National Bank ("ANB"), alleging, based on its own knowledge as to itself and its own actions and based on information and belief as to all other matters, as follows:

PARTIES

1. Textile Computer Systems, Inc. is a corporation formed under the laws of the State of Texas, with a place of business at 6517 Springwood Court, Temple, Texas, 76502.

2. Amarillo National Bank is a national bank with places of business in the Austin, Texas area and in the San Antonio, Texas area.

3. Amarillo National Bank and its affiliates lead and are part of an interrelated group of companies which together comprise one of the country's largest banking and financial service entities, including under the Amarillo National Bank brand.

4. Amarillo National Bank and its affiliates are part of the same corporate structure for the making, offering, and using of the accused instrumentalities in the United States, including in the State of Texas generally and this judicial district in particular.

5. Amarillo National Bank and its affiliates have common ownership and share advertising platforms, facilities, systems, and platforms, and accused instrumentalities and instrumentalities involving related technologies.

6. Amarillo National Bank and its affiliates regularly contract with customers and other financial institutions and payment networks regarding equipment or services that will be provided by their affiliates on their behalf.

7. Thus, Amarillo National Bank and its affiliates operate as a unitary business venture and are jointly and severally liable for the acts of patent infringement alleged herein.

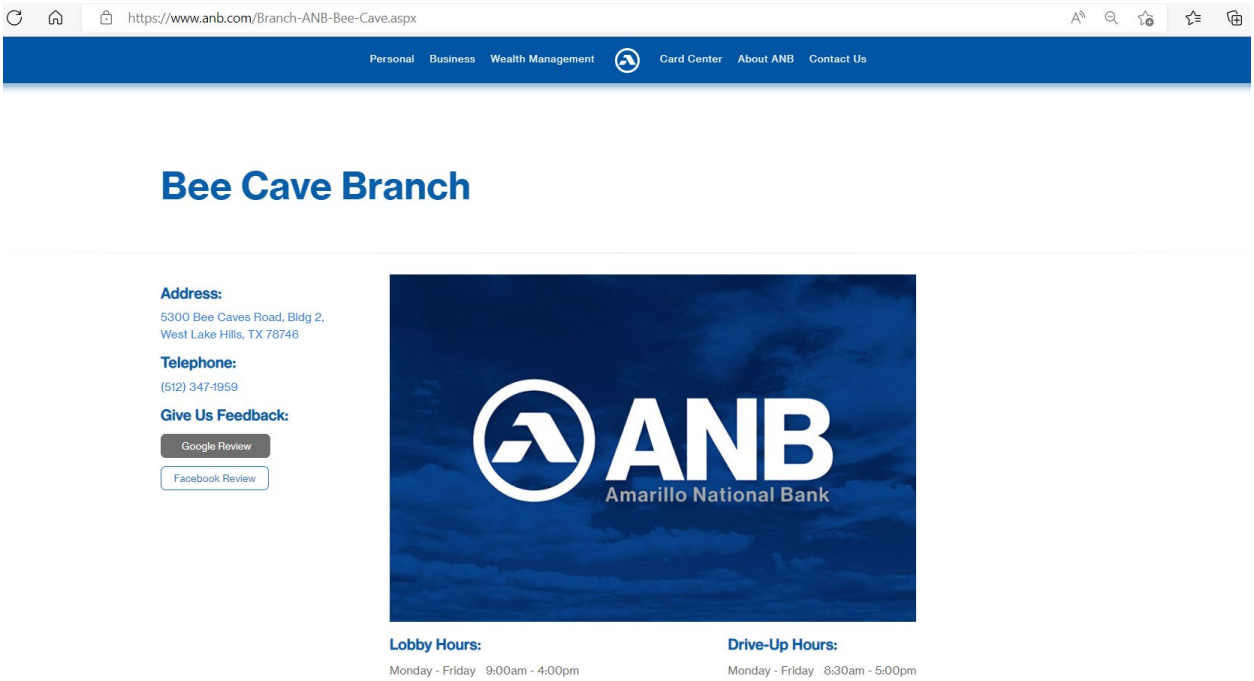
JURISDICTION AND VENUE

8. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

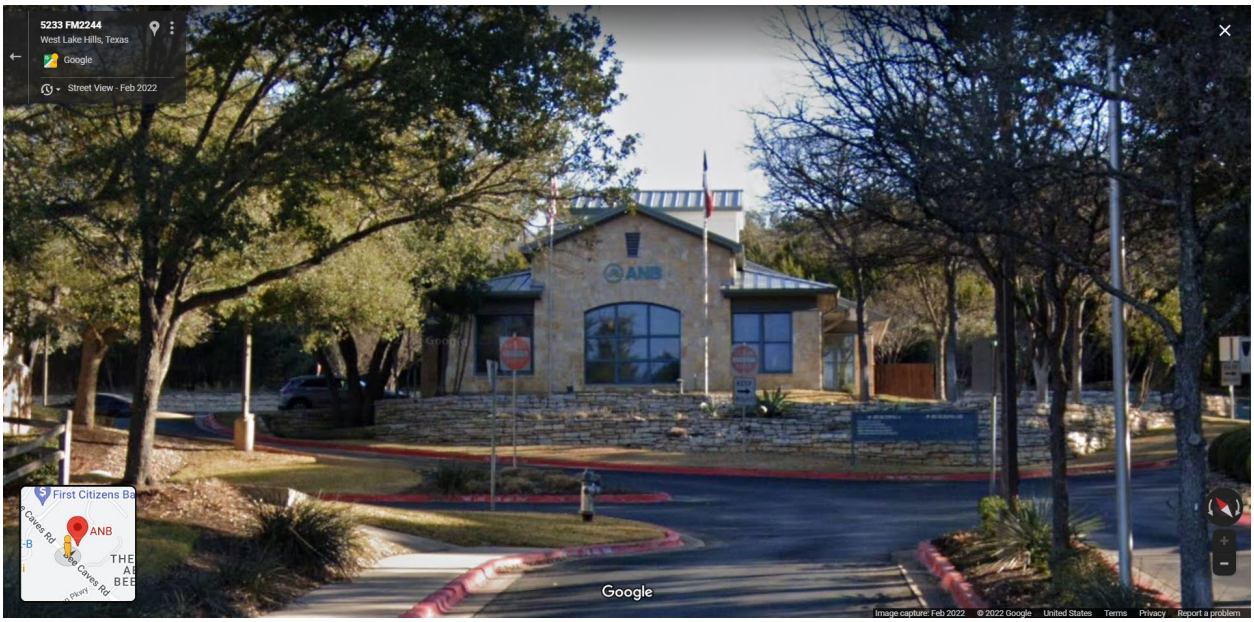
9. This Court has personal jurisdiction over ANB pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) ANB has done and continues to do business in Texas; and (ii) ANB has committed and continues to commit acts of patent infringement in the State of Texas, including making and/or using the accused instrumentality in Texas, including by Internet and via branch offices and other branch locations, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b). Venue is further proper because ANB has committed and continues to commit acts of patent infringement in this district. For example, ANB cardholders are issued debit and/or credit cards, and through using those debit and/or credit cards with certain digital payment systems, those cardholders make

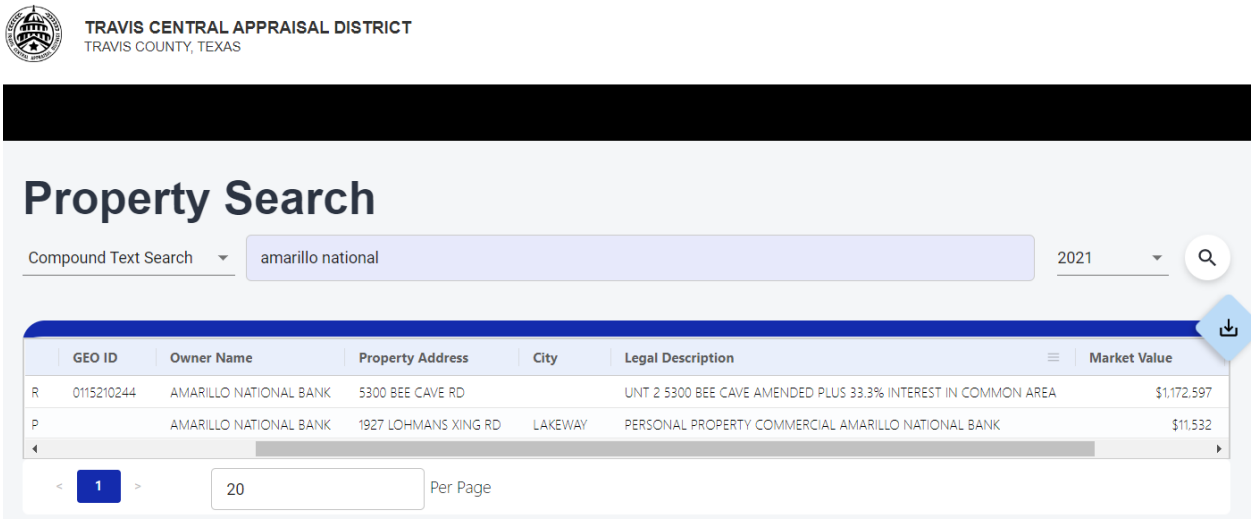
and/or use the accused instrumentalities in the district. ANB induces others to commit acts of patent infringement in Texas, and/or commit at least a portion of any other infringements alleged herein in this district. ANB has regular and established places of business in this district, including at least at 5300 Bee Caves Road, Bldg 2, West Lake Hills, TX 78746:



(Source: https://www.anb.com/Branch-ANB-Bee-Cave.aspx)



(Source: screenshot from Google Maps Street View)



(Source: screenshot from Travis CAD Property Search website)

BACKGROUND

11. The patents-in-suit generally pertain to payment authorization technology used in payment networks used to process transactions from, for example, credit cards and debit cards. The technology disclosed by the patents was developed by Gopal Nandakumar, a Texas-based entrepreneur, software engineer, and prolific inventor with over 30 years of experience in the field of Information Management Systems.

12. In 1987, after receiving Master's Degrees from both the University of Madras, India and the Georgia Institute of Technology, Mr. Nandakumar formed Textile Computer Systems, Inc. ("Textile") for the purpose of consulting and developing software for the textile industry. In 2005, Textile began transitioning into credit card transaction systems. In 2011, Textile began to develop and market the MySingleLink suite of applications.

13. The Nandakumar patents are related to payment authorization technology. Mr. Nandakumar has been at the forefront of payment authorization, developing, disclosing, and patenting solutions for reducing fraud in credit and debit card transactions. Indeed, the

Nandakumar patents (or the applications leading to them) have been cited during patent prosecution over a hundred times, including by numerous leading companies in the payment authorization industry such as ADP, Bank of America, Google, Groupon, IBM, Mastercard, NEC, Paypal, Visa, and Wells Fargo.

THE TECHNOLOGY

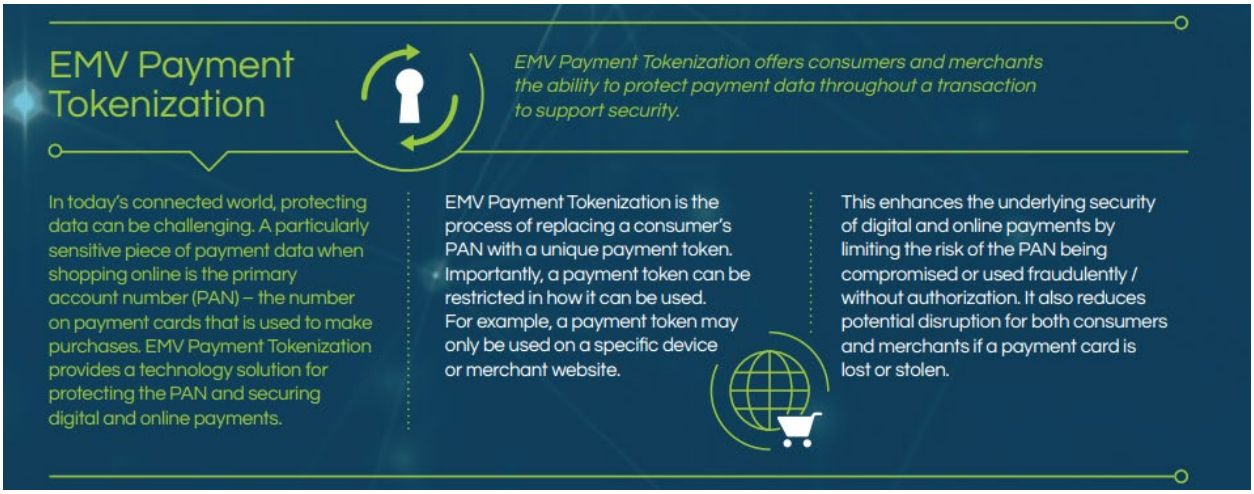
14. The patents-in-suit, U.S. Patent Nos. 8,505,079, 8,533,802, 10,148,659, and 10,560,454 (collectively, the "Asserted Patents"), teach systems, including payment processing systems, for securely and effectively approving and processing specific credit card and/or debit card transactions. Through the specific use of servers, messaging gateways, and/or interfaces, these systems act to reduce credit card and/or debit card fraud and misuse through their use and validation of key strings, authentication credentials, transaction specific information, and transaction specific credentials. The technology in the Asserted Patents improves the underlying functionality of existing card processing infrastructure by minimizing fraud and data theft in the face of attacks on payment systems that continue to grow in their number and sophistication.

15. The patented improvements are critical for implementing secure payment systems, especially in light of the many high-profile merchant data breaches that have led to increased credit and debit card fraud. For example, in 2006, TJX Companies, who owns retailers like TJMaxx and Marshall's, was hit with a cyber attack that resulted in the theft of credit cards leading to over $100 million in fraud losses. In 2013, five people were indicted for attacking a number of retailers and financial institutions including NASDAQ, 7-Eleven, JCP, and others, stealing over 160 million cards. Also in 2013, the retailer Target suffered a data breach that resulted in 40 million debit and credit cards being compromised.

16. One implementation of the technology claimed in the Asserted Patents has been described by EMVCo as "a global Payment Tokenisation ecosystem that overlays and interoperates with existing payment ecosystems to support digital commerce and new methods of payment" and as "enhanc[ing] the underlying security of digital payments by potentially limiting the risk typically associated with compromised, unauthorized or fraudulent use of PANs." (Source: https://www.emvco.com/emv-technologies/payment-tokenisation/).

17. The technology claimed in the Asserted Patents is far from conventional technology. The payment industry gathered and consulted experts who worked together over a number of years to develop infringing payment tokenisation systems. In other words, the technology claimed in the Asserted Patents was not existing or conventional technology that the payment industry had sitting on the shelf.

18. Indeed, as recently as February of this year, EMVCo itself recognized that an implementation of the technology claimed in the Asserted Patents "provides a technology solution for protecting the PAN and securing digital and online payments":



(Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

19. That same EMVCo document notes that "In today's connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases" and that EMVCo's payment tokenization "enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorization." The document also states that the "Payment Tokenisation Specification provides an interoperable Technical Framework." (Source: https://www.emvco.com/wp-content/uploads/documents/Quick-Resource_How-EMV-Specifications-Support-Online-Commerce.pdf)

20. One of the asserted patents, the 079 Patent, was challenged in an Inter Partes Review proceeding before the Patent and Trademark Office ("PTO"). The PTO found that the challenger, Unified Patents Inc., was unable to show that one element, the "key string" as claimed in the 079 Patent claims and as construed by the PTO, was in the prior art at all, much less it being conventional or widespread. The PTO thus confirmed the patentability of all challenged claims of the 079 Patent.

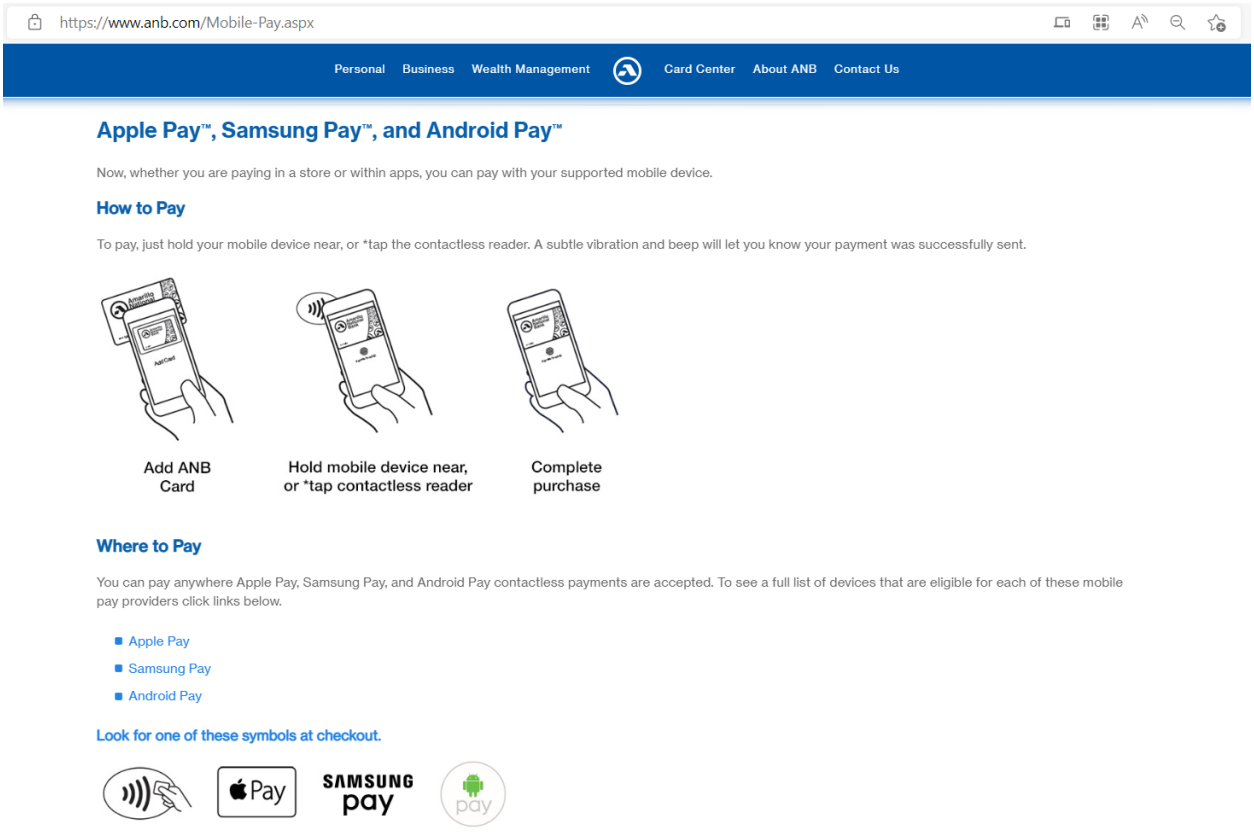
COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,505,079

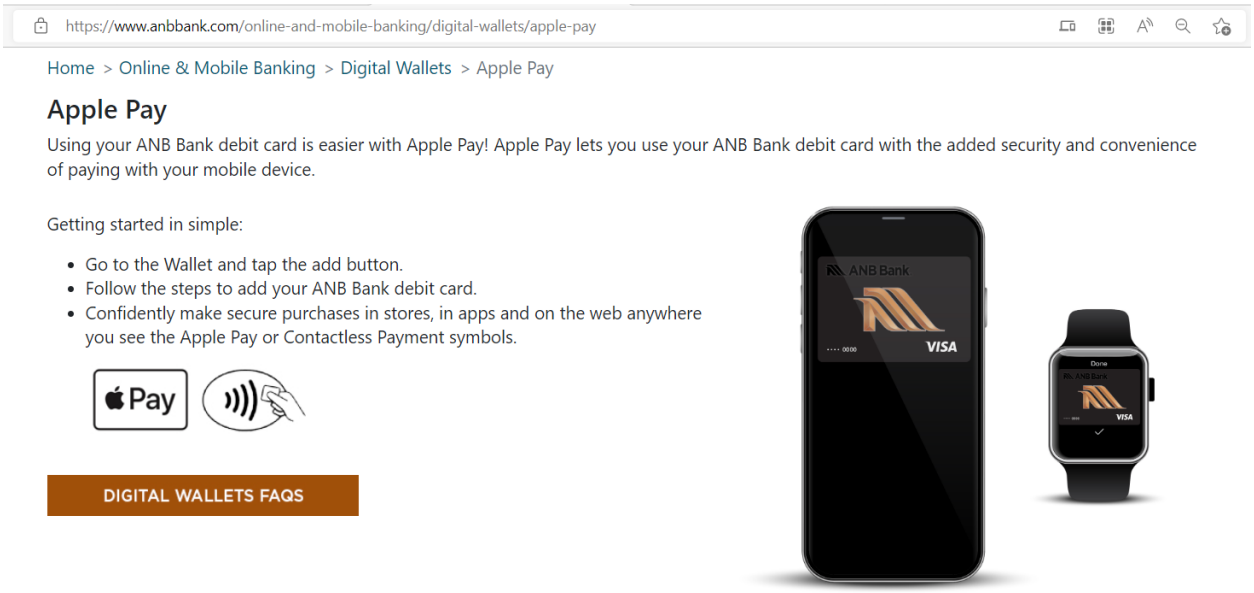
21. On August 6, 2013, United States Patent No. 8,505,079 ("the 079 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Related Method."

22. Textile is the owner of the 079 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 079 Patent against infringers, and to collect damages for all relevant times.

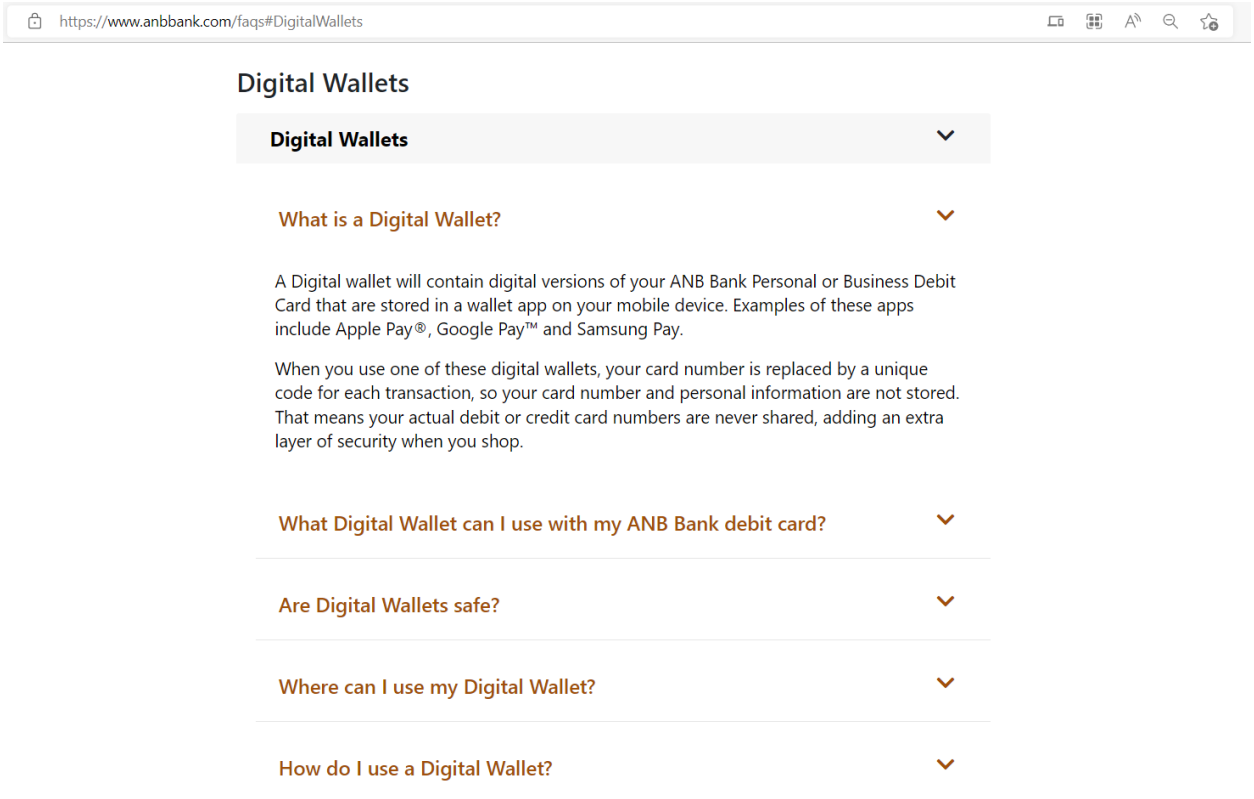
23. ANB offers debit and/or credit cards, such as the ANB Visa Debit Cards, that are used with an ANB authentication system that authenticates the identity of a ANB card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). The ANB card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities, for example. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



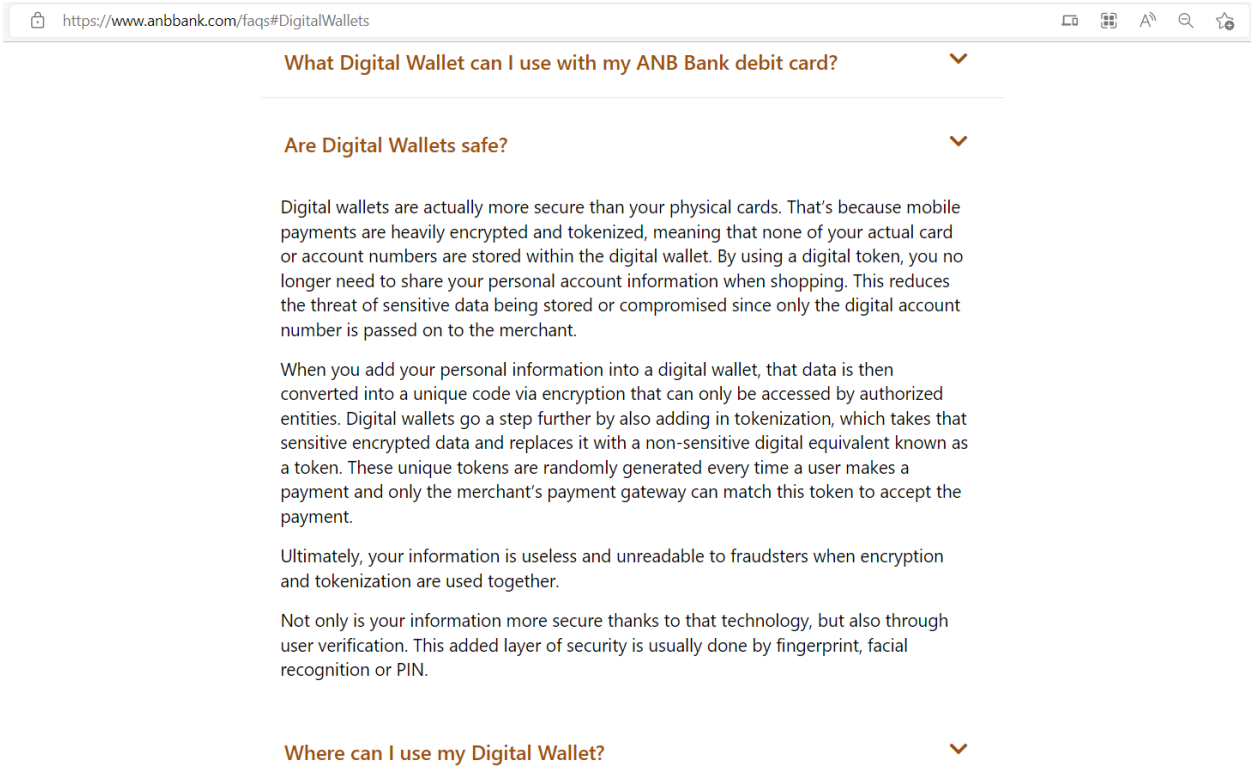
(Source: https://www.anb.com/Mobile-Pay.aspx)



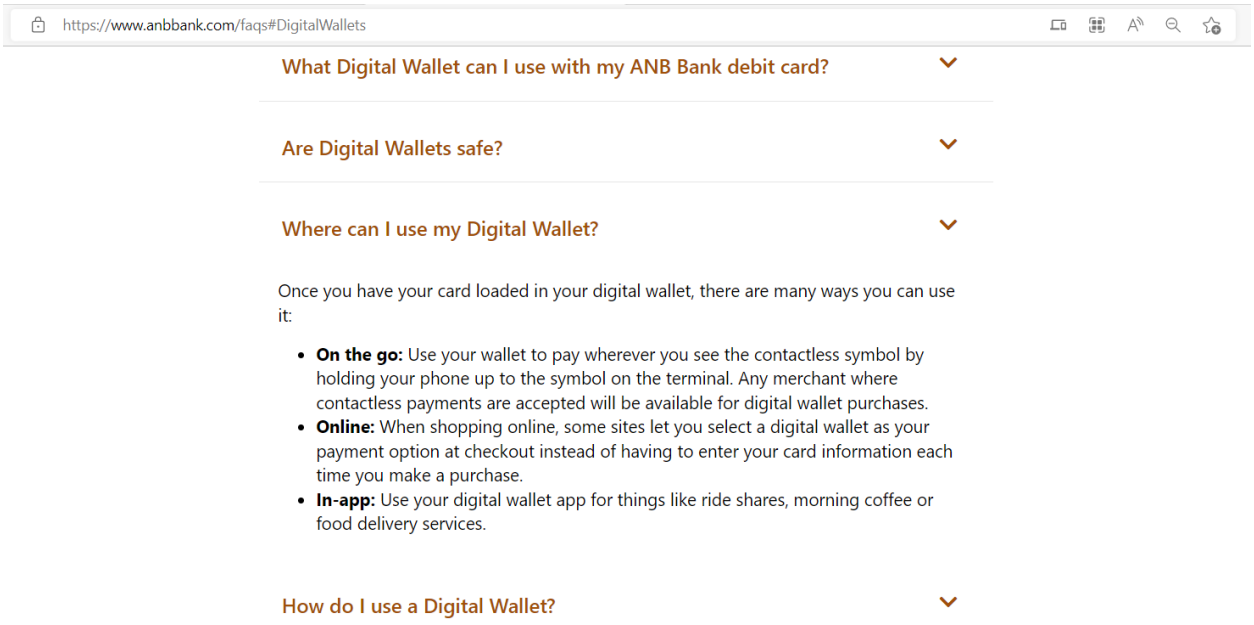
(Source: https://www.anbbank.com/online-and-mobile-banking/digital-wallets/apple-pay)



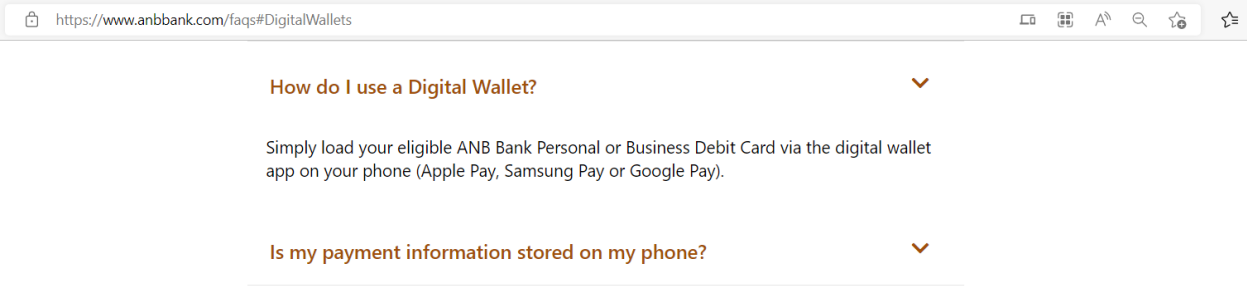
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)



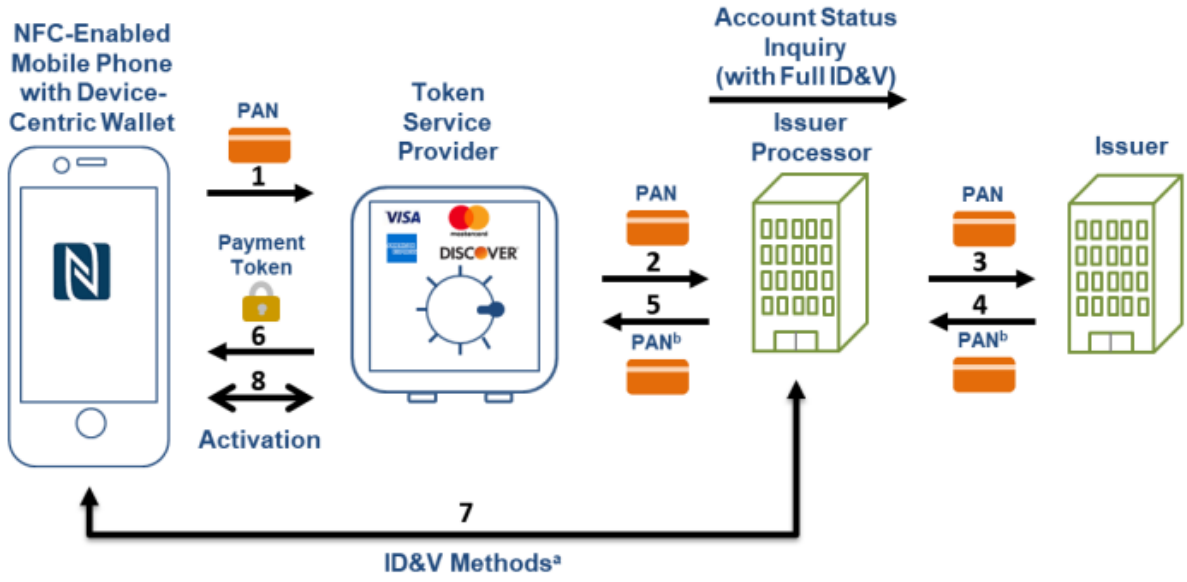
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

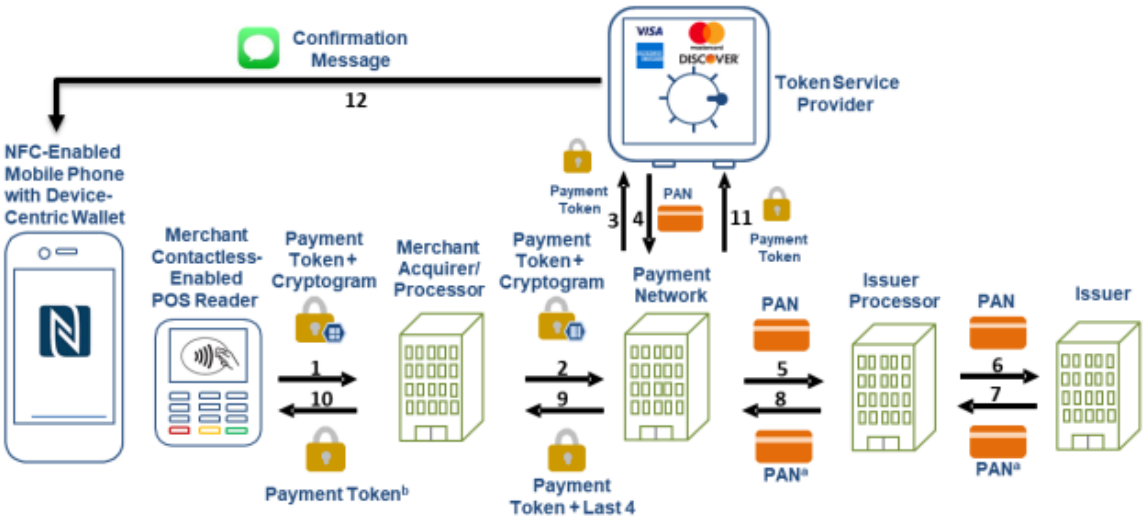
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

24. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a ANB account holder requests ANB to provision a specific ANB debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives

certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

25. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by ANB card account holders for provisioning a specific ANB debit and/or credit card for use on their mobile devices. The messaging gateway is also programmed to receive requests initiated by ANB card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder. This messaging gateway is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

26. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the messaging

gateway and in secure communication therewith is an authorization server that processes the received request to identify the token value sent for the account selected to be charged that was passed from the authorized user to the merchant terminal via the NFC communication link. From the token value, the server can look up the debit and/or credit card account number. The authorization server is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

27. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive within the payment authorization request transaction specific information that was input into the request by the merchant. The interface is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

28. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

29. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

30. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

31. Defendants thus infringe one or more of the claims of the 079 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 079 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 079 Patent.

32. ANB has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(a), by making, using, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

33. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 079 Patent by others and ANB will continue to do so unless enjoined by this Court. ANB's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 079 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. ANB knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 079 Patent.

34. ANB continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 079 Patent.

35. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 079 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 079 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. ANB has committed these acts of infringement without license or authorization.

37. By engaging in the conduct described herein, ANB has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and ANB is thus liable to Textile for infringement of the 079 Patent, pursuant to 35 U.S.C. § 271.

38. As a direct and proximate result of ANB's infringement of the 079 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for ANB's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

39. In addition, the infringing acts and practices of ANB have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which ANB is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that ANB is finally and permanently enjoined from further infringement.

40. ANB has had actual knowledge of the 079 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, ANB will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 079 Patent.

41. ANB has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 079 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

42. Textile has been damaged as a result of the infringing conduct by ANB alleged above. Thus, ANB is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

43. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 079 Patent.

COUNT II

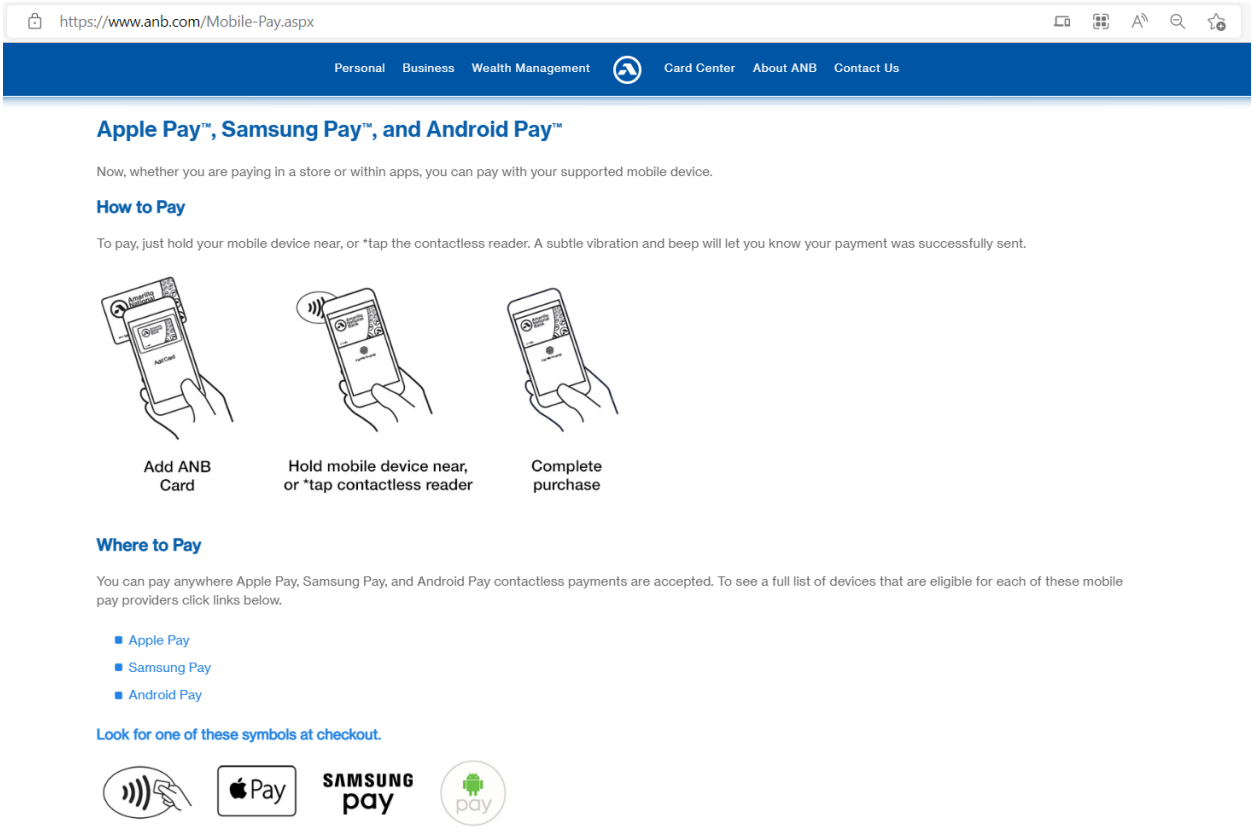
INFRINGEMENT OF U.S. PATENT NO. 8,533,802

44. On September 10, 2013, United States Patent No. 8,533,802 ("the 802 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Related Method."

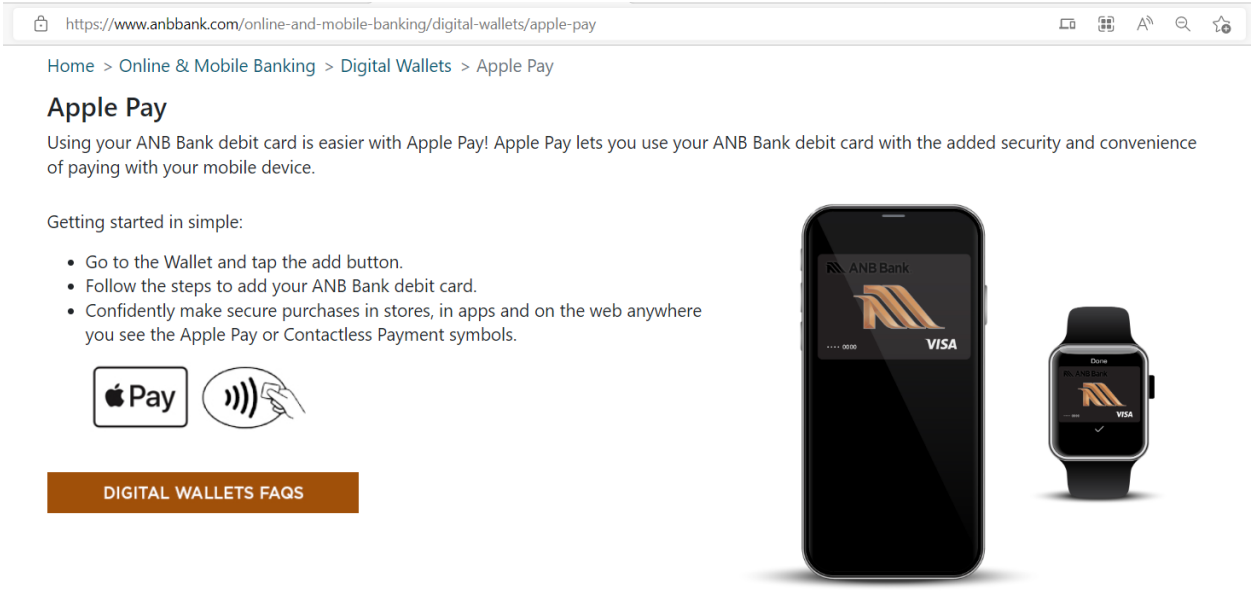
45. Textile is the owner of the 802 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 802 Patent against infringers, and to collect damages for all relevant times.

46. ANB offers debit and/or credit cards, such as the ANB Visa Debit Cards, that are used with an ANB authentication system that authenticates the identity of a ANB card holder in a request to pay a merchant for a transaction (the "Accused Instrumentality"). The ANB card authentication system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated

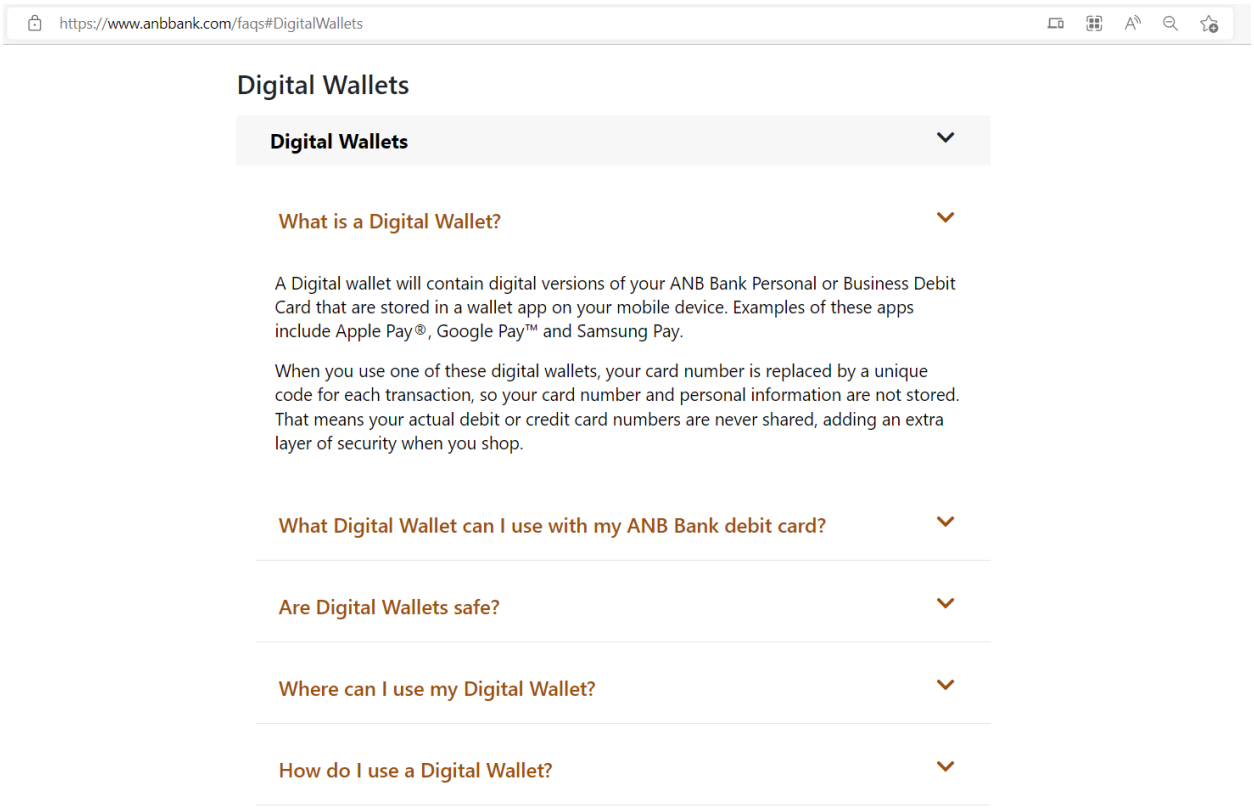
and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



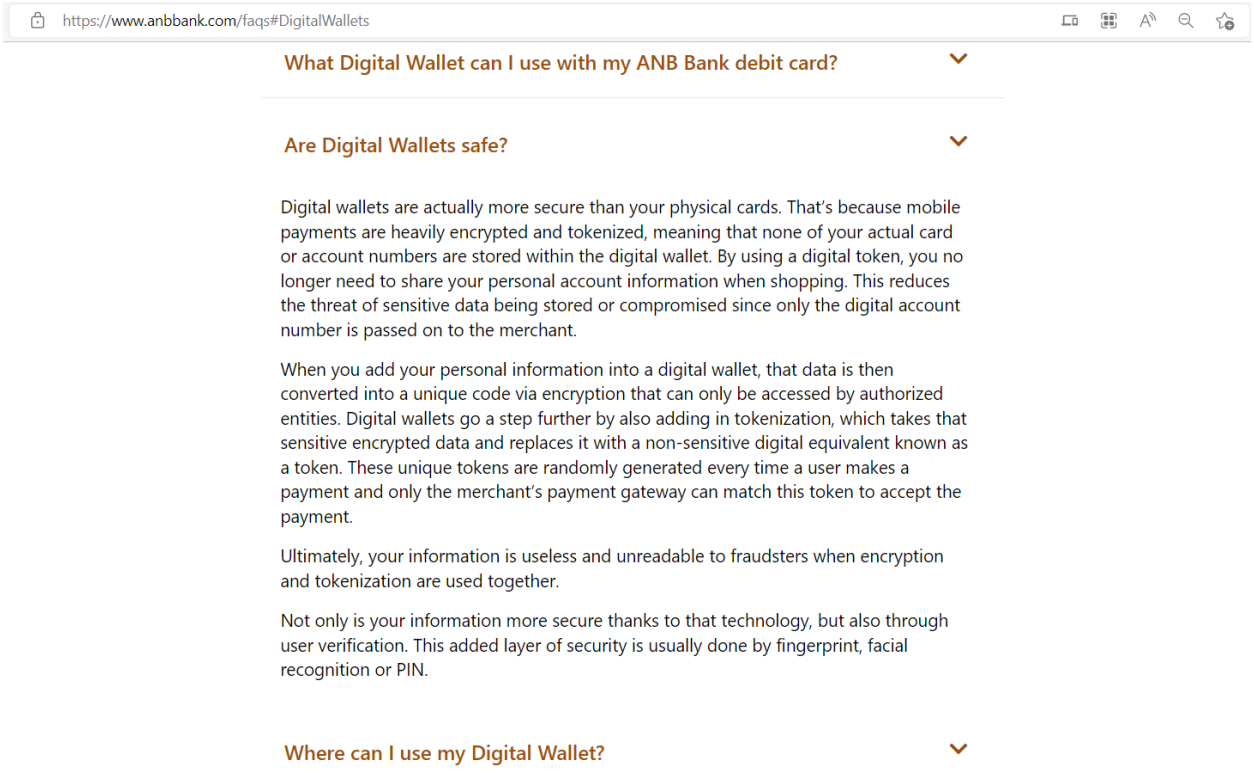
(Source: https://www.anb.com/Mobile-Pay.aspx)



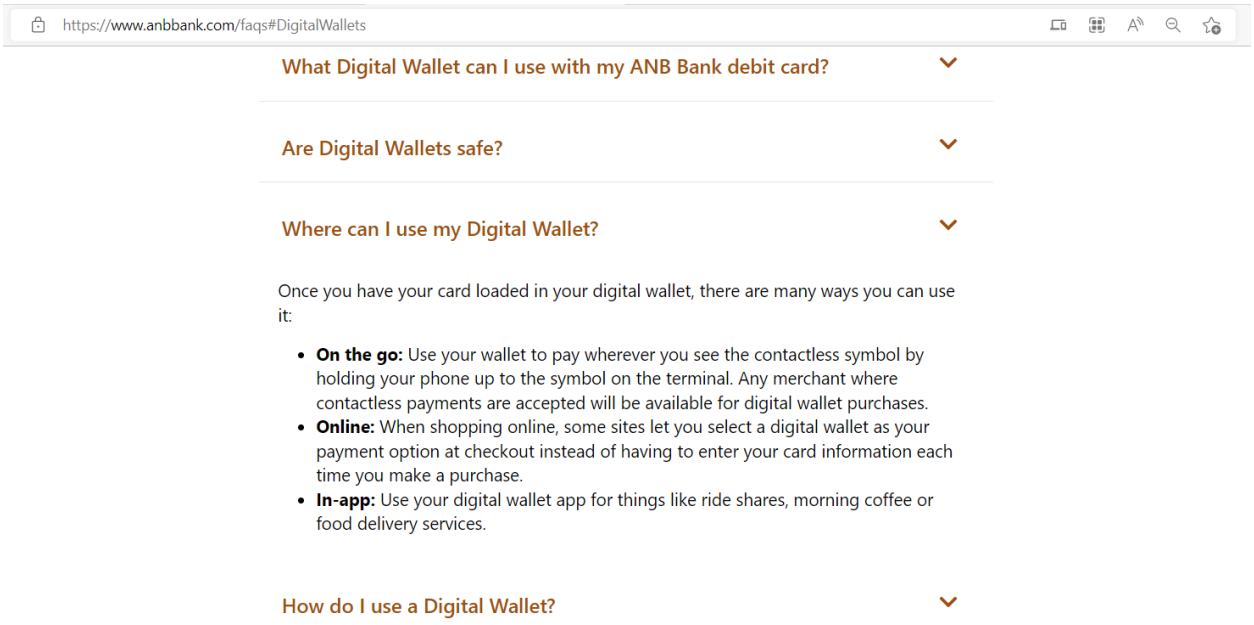
(Source: https://www.anbbank.com/online-and-mobile-banking/digital-wallets/apple-pay)



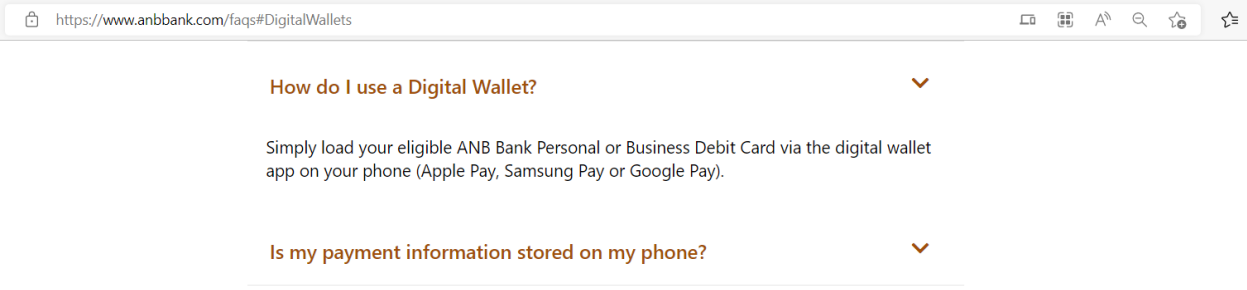
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)



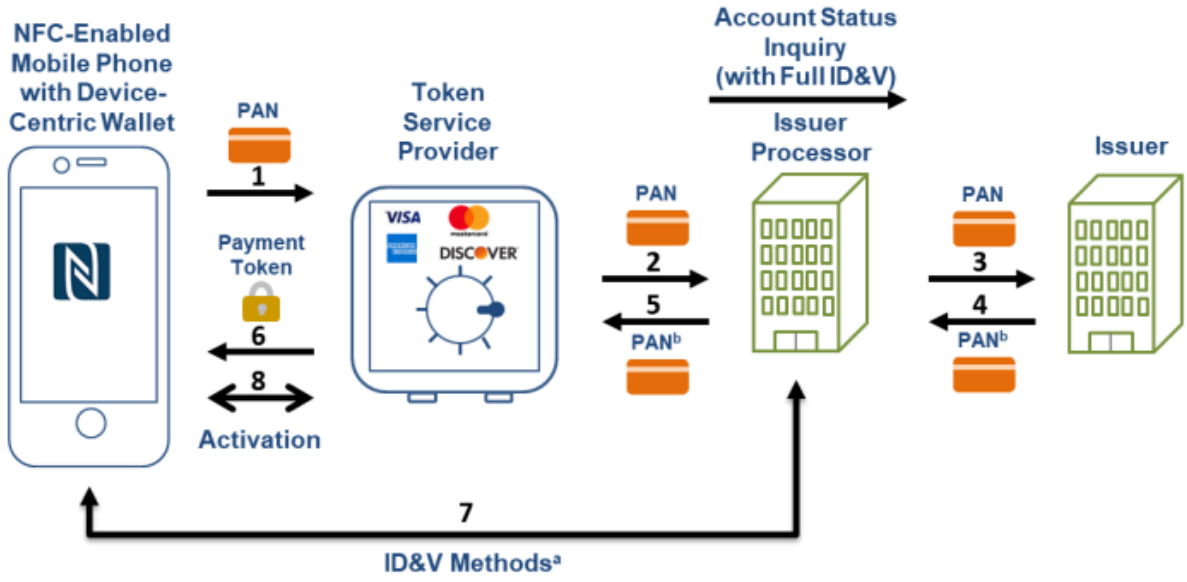
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

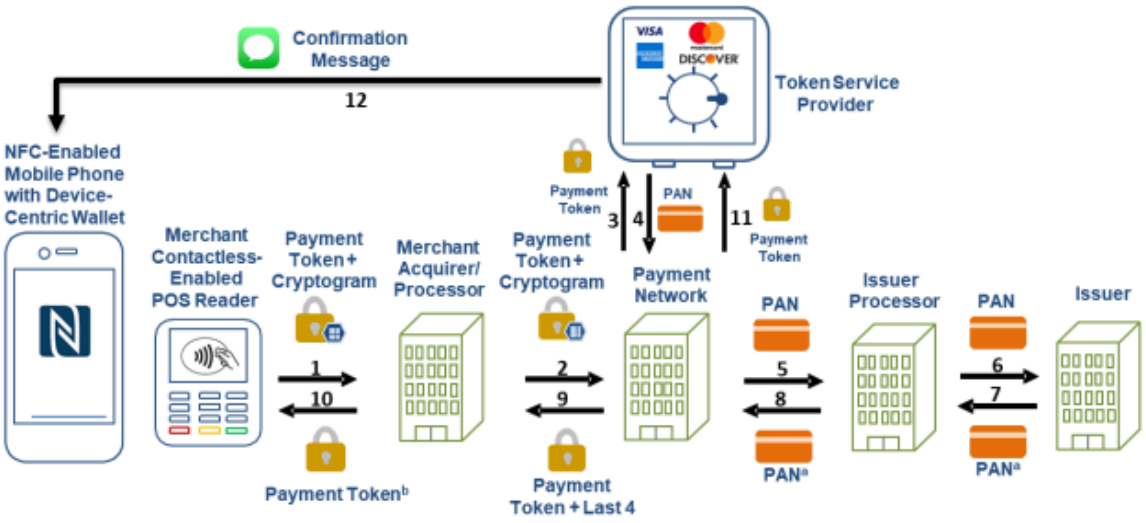
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

47. The Accused Instrumentality includes an authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource. For example, a ANB account holder requests ANB to provision a specific ANB debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives

certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent, some of which was used in making the cryptogram.

48. The Accused Instrumentality comprises a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource. For example, the Accused Instrumentality includes a messaging gateway that is programmed to receive requests initiated by ANB card account holders for provisioning a specific ANB debit and/or credit card for use on their mobile devices. This messaging gateway is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

49. The Accused Instrumentality includes a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to generate a key string adapted to provide a basis for authenticating the identity of said requester. For example, behind the firewall of the message gateway and in secure communication therewith is an authorization server that generates a token corresponding to the debit and/or credit card account number. The authorization server is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

50. The Accused Instrumentality includes a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client. For example, the authorization server includes an interface with programming instructions to also receive transaction specific information that was input into the request by the merchant, *e.g.*, the merchant ID, invoice number, invoice amount, and date/timestamp. The interface is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

51. The Accused Instrumentality includes a first set of instructions further operable to communicate the key string to the authorized user that the requester purports to be. For example, the messaging gateway sends the generated token to the authorized user's mobile device for use in merchant transactions.

52. The Accused Instrumentality includes a second set of instructions further operable to receive an authentication credential from said unauthorized service client, said authentication credential having been provided to said unauthorized service client by said requester. For example, the authorization server is also programmed to identify within the payment authorization request the cryptogram that was passed by the user to the merchant and the authorization server will use the cryptogram to authenticate that the request originated with the actual account holder.

53. The Accused Instrumentality includes a second set of instructions further operable to evaluate said authentication credential to authenticate the identity of said requestor. For example, the authorization server uses the token value and other transaction information received

to evaluate the cryptogram. If the cryptogram is valid, the authorization server authenticates the identity of requestor as the actual account holder.

54. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

55. Defendants thus infringe one or more claims of the 802 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 1 of the 802 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 802 Patents.

56. ANB has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

57. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 802 Patent by others and ANB will continue to do so unless enjoined by this Court. ANB's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors,

agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 802 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. ANB knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 802 Patent.

58. ANB continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 802 Patent.

59. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 1 of the 802 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 802 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

60. ANB has committed these acts of infringement without license or authorization.

61. By engaging in the conduct described herein, ANB has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and ANB is thus liable to Textile for infringement of the 802 Patent, pursuant to 35 U.S.C. § 271.

62. As a direct and proximate result of ANB's infringement of the 802 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for ANB's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

63. In addition, the infringing acts and practices of ANB have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which ANB is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that ANB is finally and permanently enjoined from further infringement.

64. ANB has had actual knowledge of the 802 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, ANB will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 802 Patent.

65. ANB has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 802 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

66. Textile has been damaged as a result of the infringing conduct by ANB alleged above. Thus, ANB is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 802 Patent.

COUNT III

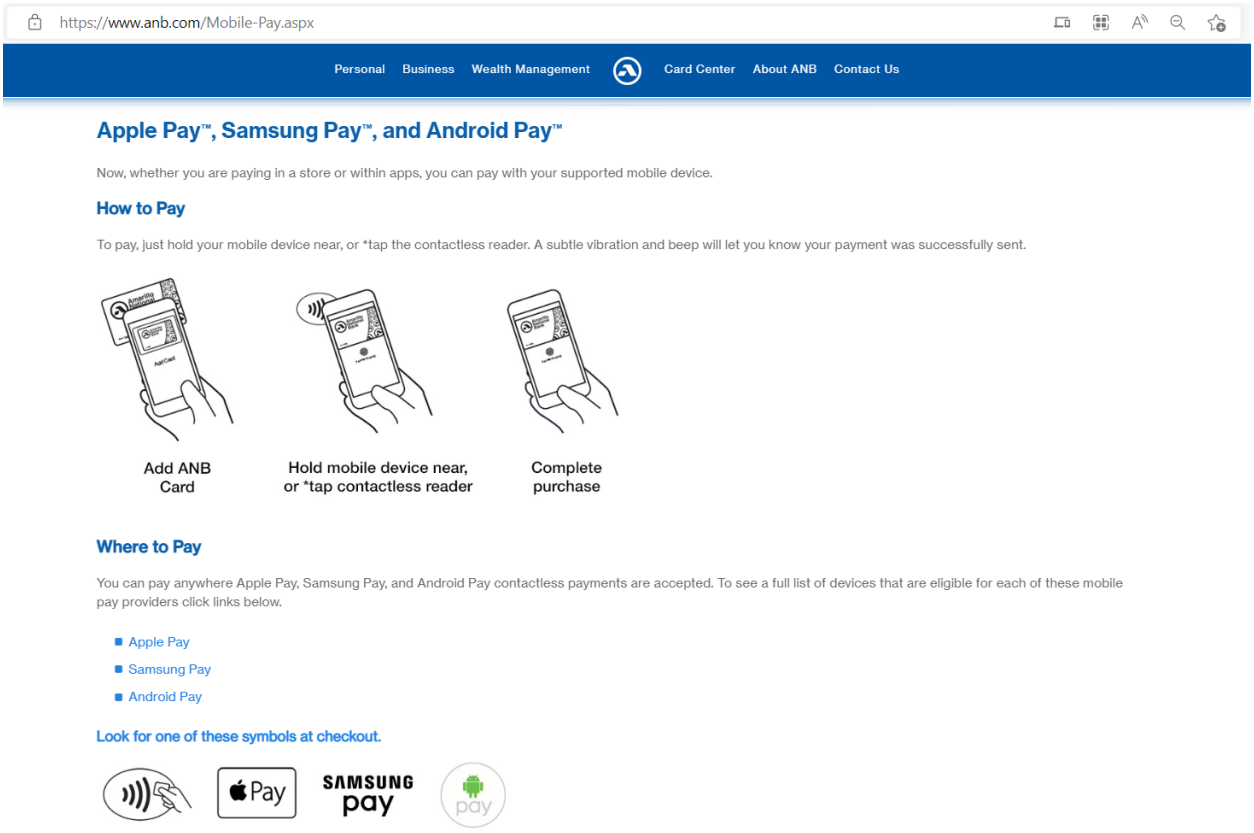
INFRINGEMENT OF U.S. PATENT NO. 10,148,659

68. On December 4, 2018, United States Patent No. 10,148,659 ("the 659 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Method."

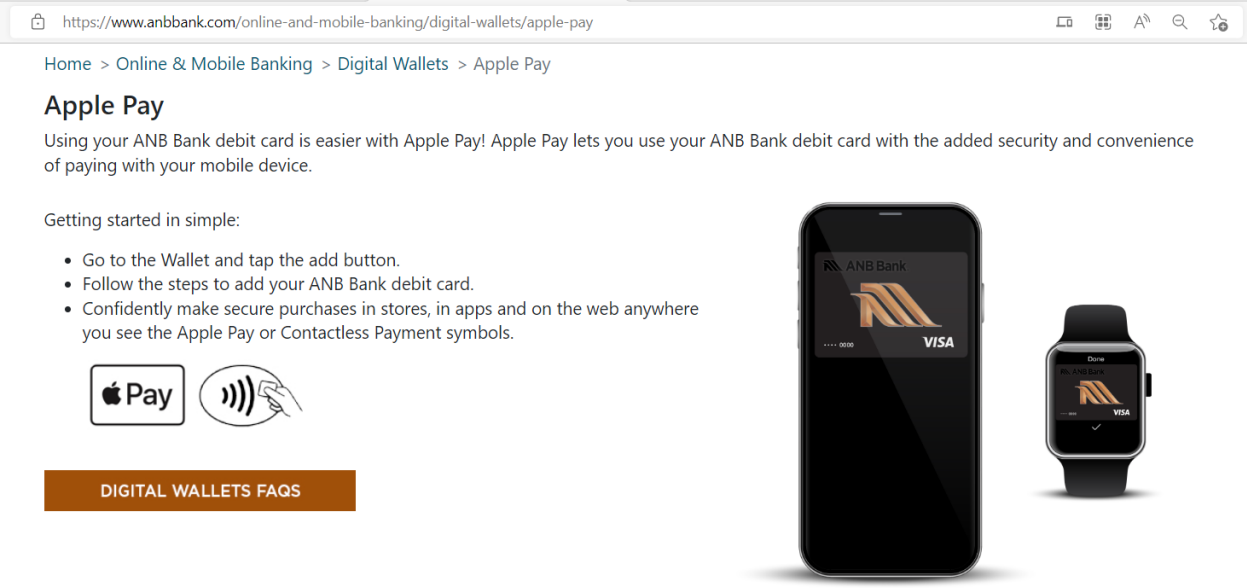
69. Textile is the owner of the 659 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 659 Patent against infringers, and to collect damages for all relevant times.

70. ANB offers debit and/or credit cards, such as the ANB Visa Debit Cards, that are used with an ANB computer-implemented system for a credit or debit and/or credit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit and/or credit card account number to the merchant (the "Accused Instrumentality"). The ANB transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account

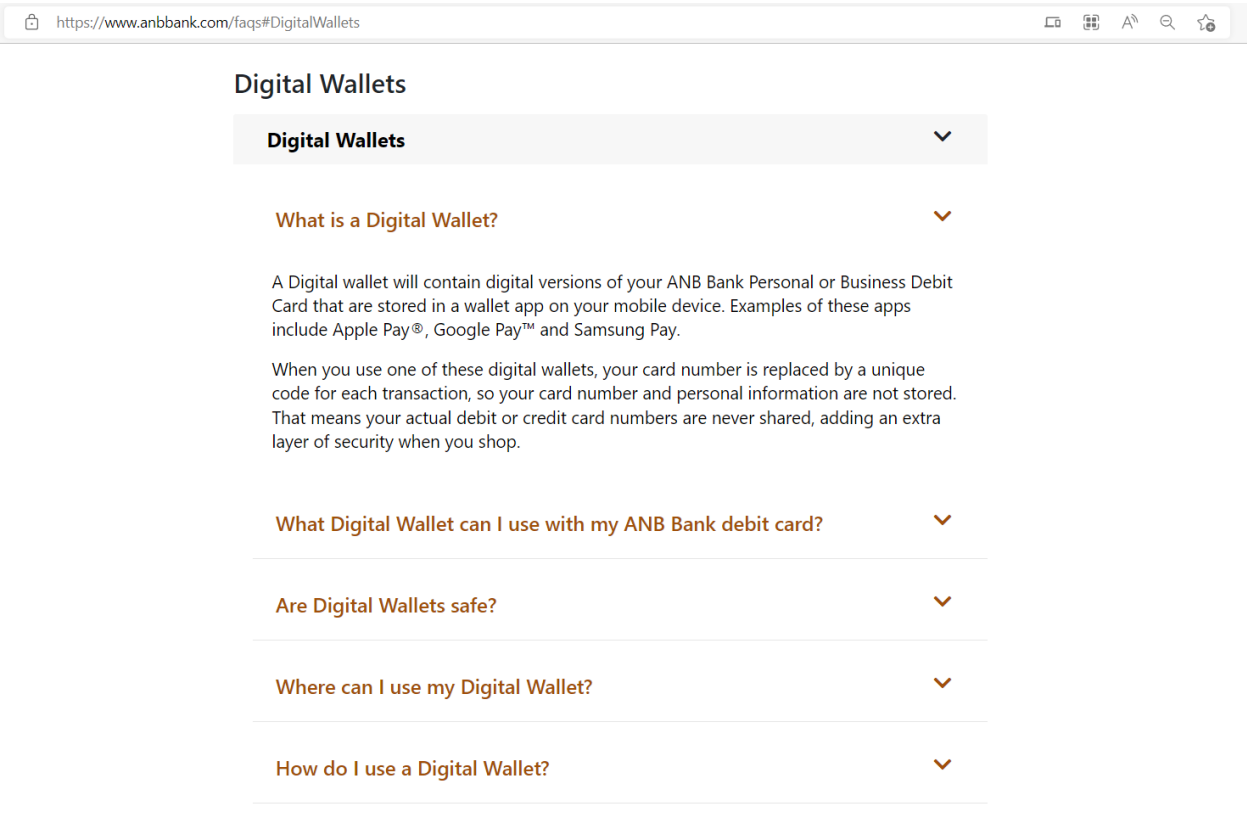
holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



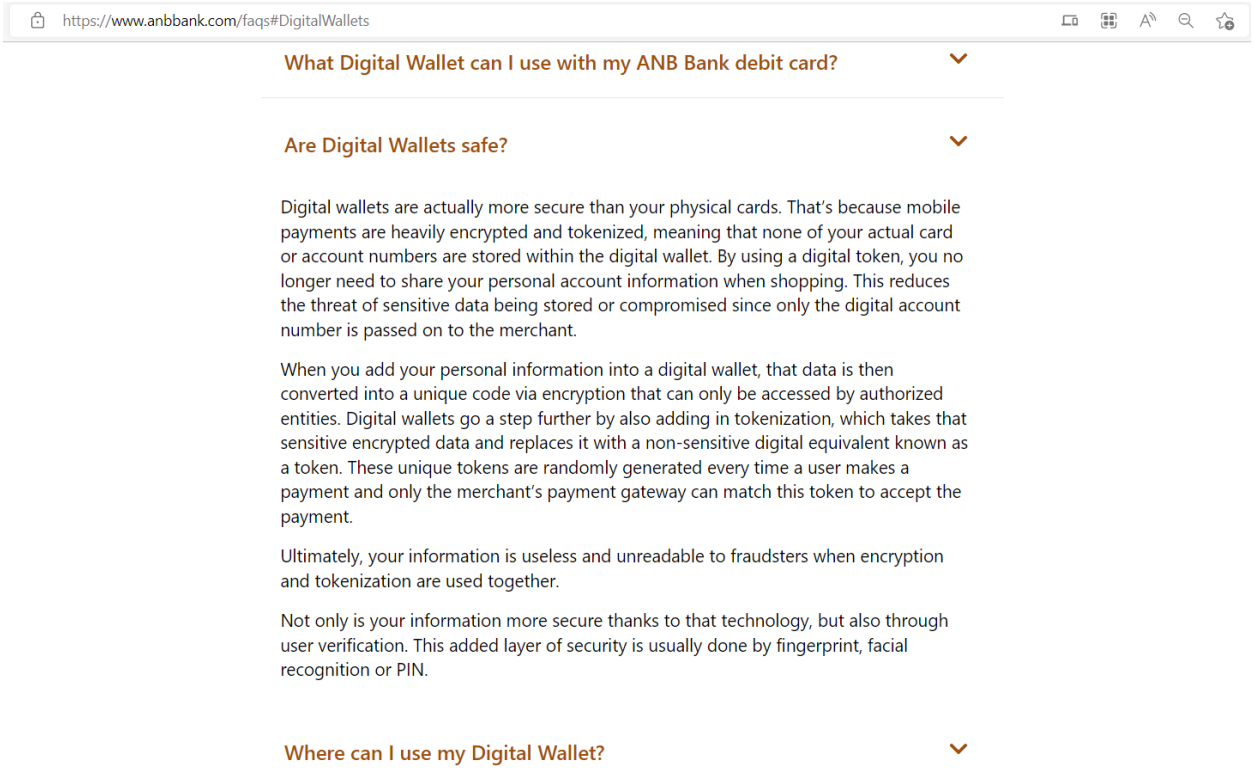
(Source: https://www.anb.com/Mobile-Pay.aspx)



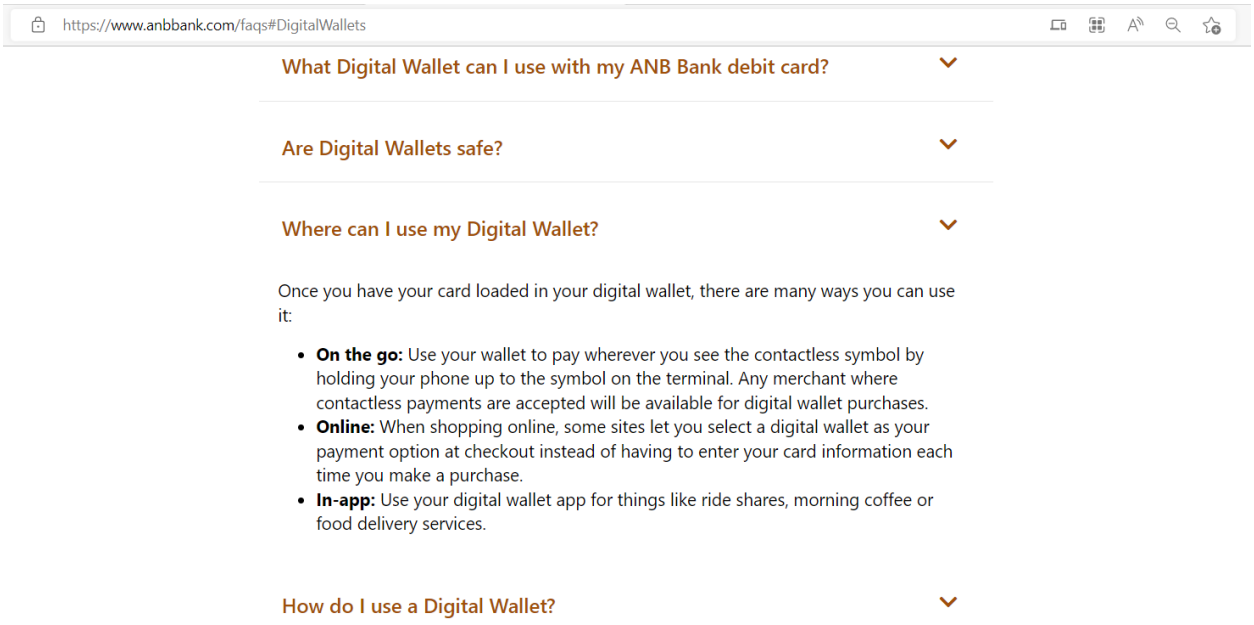
(Source: https://www.anbbank.com/online-and-mobile-banking/digital-wallets/apple-pay)



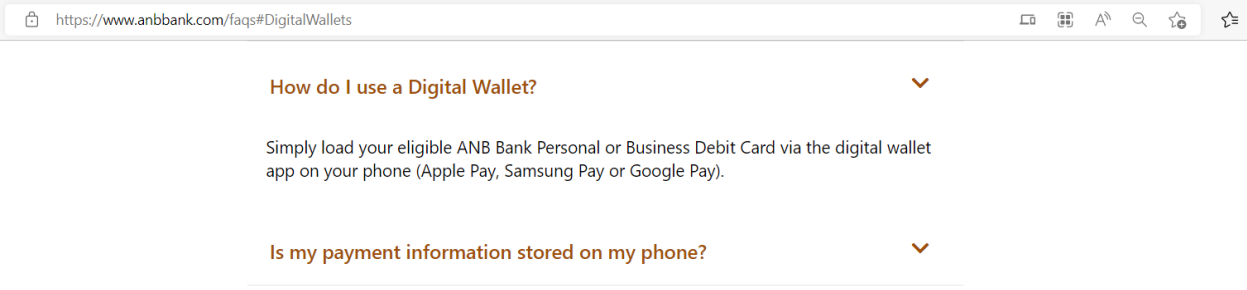
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)



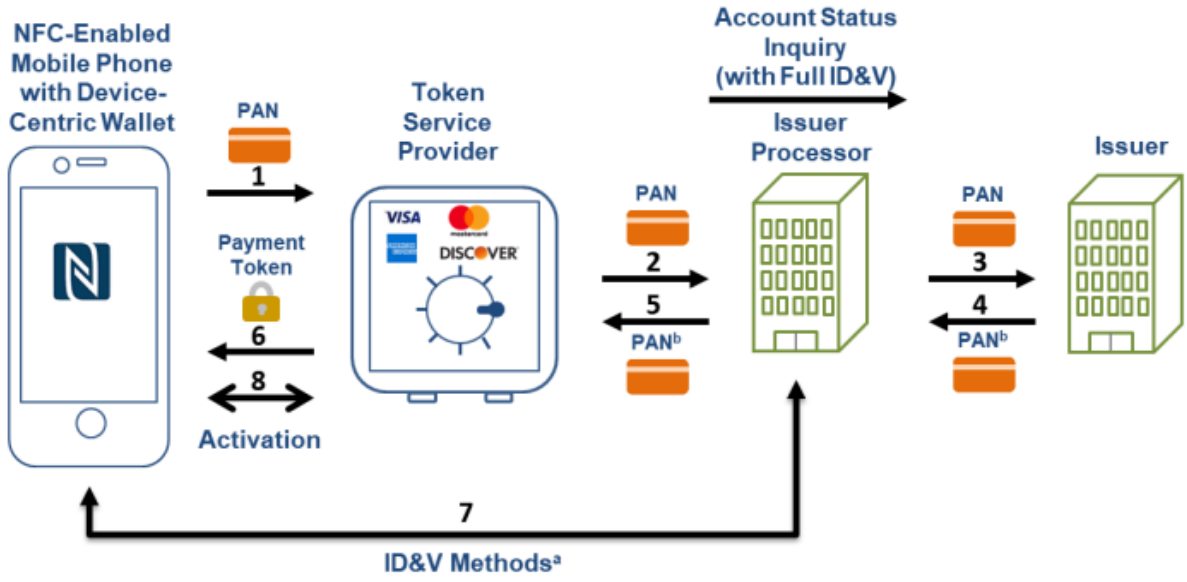
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

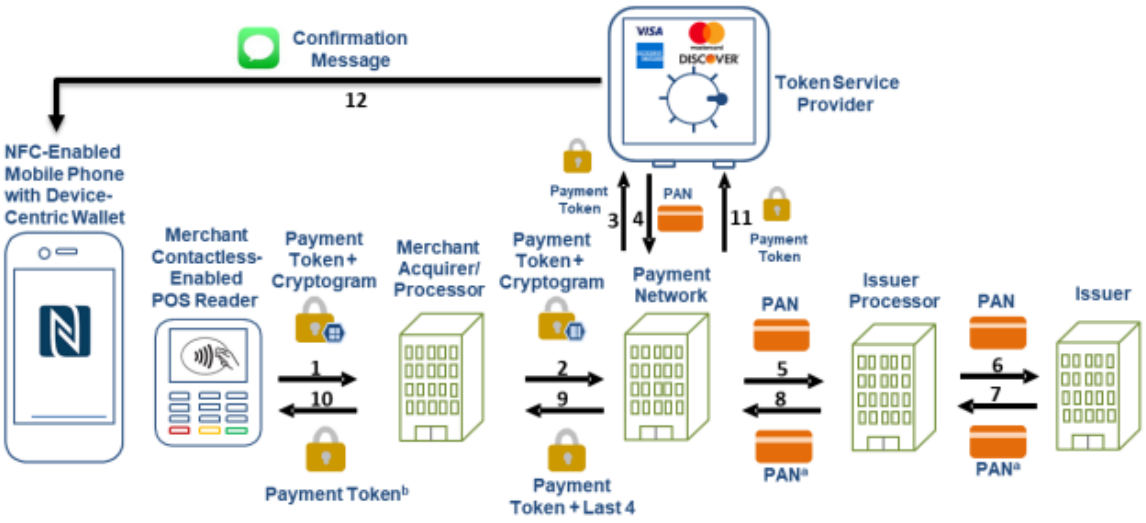
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

71. The Accused Instrumentality includes a computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant. For example, a ANB account holder requests ANB to provision a specific ANB debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by ANB to a specific merchant in a specific amount for a specific transaction from a specific ANB card

account of the account holder using his or her smartphone when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

72. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a ANB card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by ANB card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder. This interface is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

73. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration

information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card and the debit and/or credit card account number (which has a corresponding token), received from ANB card account holders through the interface for provisioning a specific ANB debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by ANB card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

74. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising: a first merchant identifier; a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier; the credit or debit card account holder identifier; and a designated unique account identifier selected from the at least one unique account identifiers. For example, the Accused

Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the ANB card account holder's mobile device. The server is programmed to receive authorization requests initiated by ANB card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction, a token, a merchant identifier, and the ANB card account holder identifier. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

75. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string wherein the key string is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

76. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising: a second merchant identifier; a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific authentication credential whereby the second authentication credential was received by the merchant application from the credit or debit card account holder's mobile device. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the ANB card account holder's mobile device. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

77. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the

specific merchant by determining if: the first merchant identifier matches the second merchant identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

78. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

79. Defendants thus infringe one or more claims of the 659 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 9 of the 659 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 659 Patent.

80. ANB has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. §

271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

81. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 659 Patent by others and ANB will continue to do so unless enjoined by this Court. ANB's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 659 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. ANB knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 659 Patent.

82. ANB continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 659 Patent.

83. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 9 of the 659 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 659 Patent by others, such as consumers,

businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

84. ANB has committed these acts of infringement without license or authorization.

85. By engaging in the conduct described herein, ANB has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and ANB is thus liable to Textile for infringement of the 659 Patent, pursuant to 35 U.S.C. § 271.

86. As a direct and proximate result of ANB's infringement of the 659 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for ANB's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

87. In addition, the infringing acts and practices of ANB have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which ANB is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that ANB is finally and permanently enjoined from further infringement.

88. ANB has had actual knowledge of the 659 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, ANB will have known and intended

(since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 659 Patent.

89. ANB has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 659 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

90. Textile has been damaged as a result of the infringing conduct by ANB alleged above. Thus, ANB is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

91. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 659 Patent.

COUNT IV

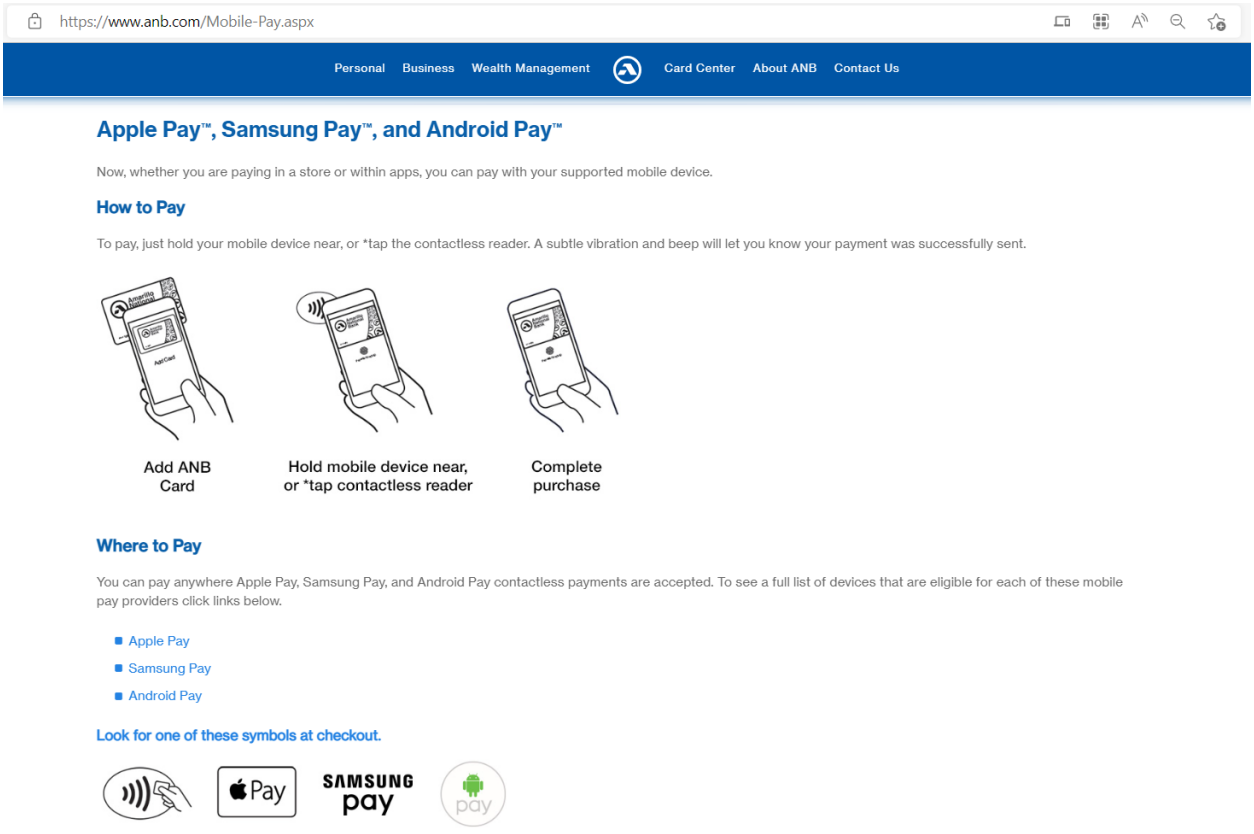
INFRINGEMENT OF U.S. PATENT NO. 10,560,454

92. On February 11, 2020, United States Patent No. 10,560,454 ("the 454 Patent") was duly and legally issued by the United States Patent and Trademark Office for an invention entitled "Authentication System and Method."

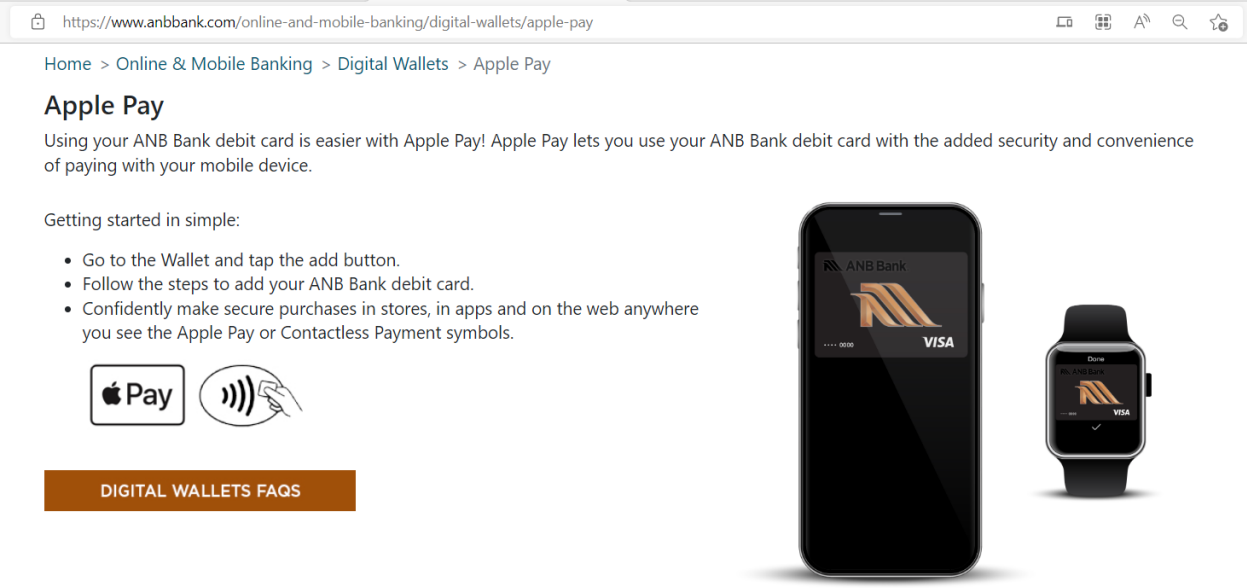
93. Textile is the owner of the 454 Patent, with all substantive rights in and to that patent, including the sole and exclusive right to prosecute this action and enforce the 454 Patent against infringers, and to collect damages for all relevant times.

94. ANB offers debit and/or credit cards, such as the ANB Visa Debit Cards, that are used with an ANB computer-implemented system for a user to authorize a resource authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service

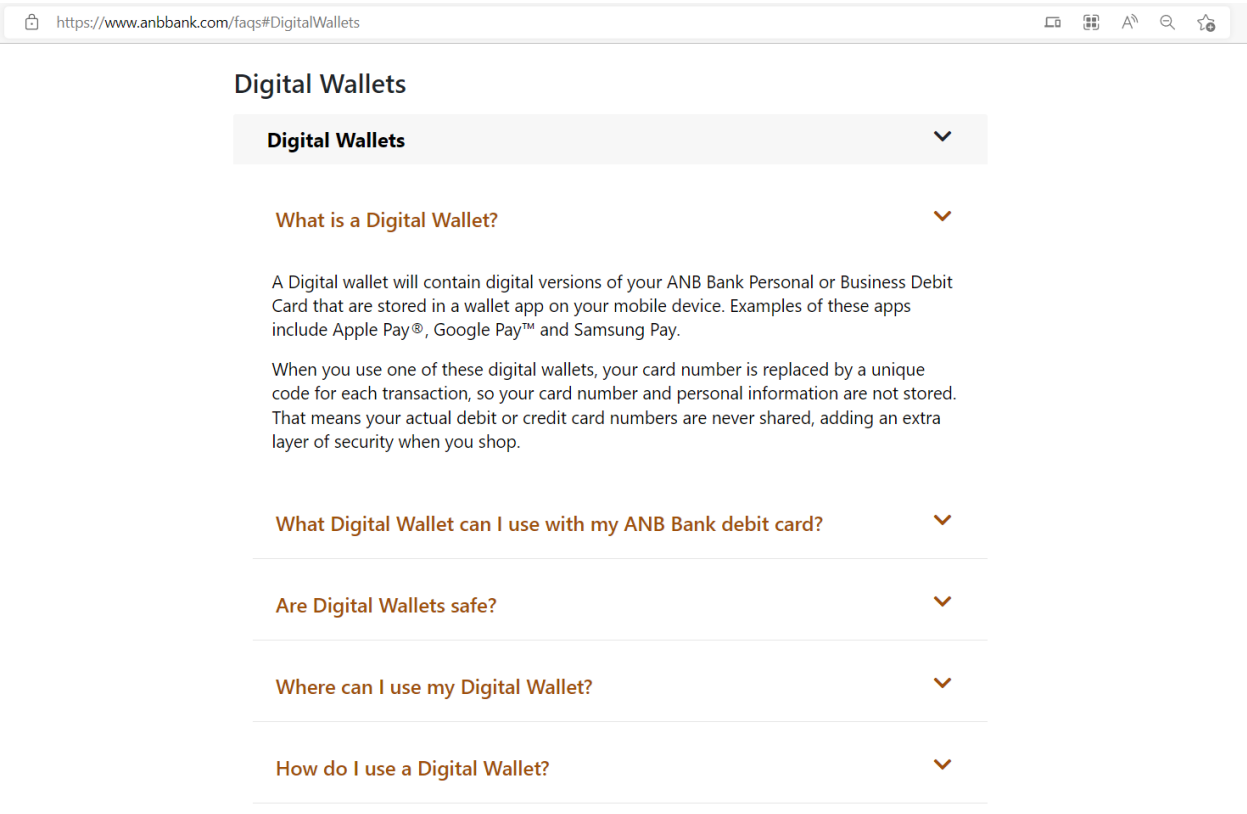
client (the "Accused Instrumentality"). The ANB transaction-specific access authorization system is implemented, in part, via EMVCo compliant tokens that are used in the transaction instead of the user's debit and/or credit card number so that the user's debit and/or credit card number is never transmitted or otherwise provided to the merchant thereby preventing the user's debit and/or credit card number from being deliberately or unintentionally transferred from the merchant to a third-party such as through hacking, spoofing, or other man-in-the-middle vulnerabilities. The requests are initiated by account holders via their smartphones, typically at an NFC (near field communication) merchant terminal and use those tokens, which are generated and communicated to the user's smartphone by the system, and wherein each account held by the user has its own token.



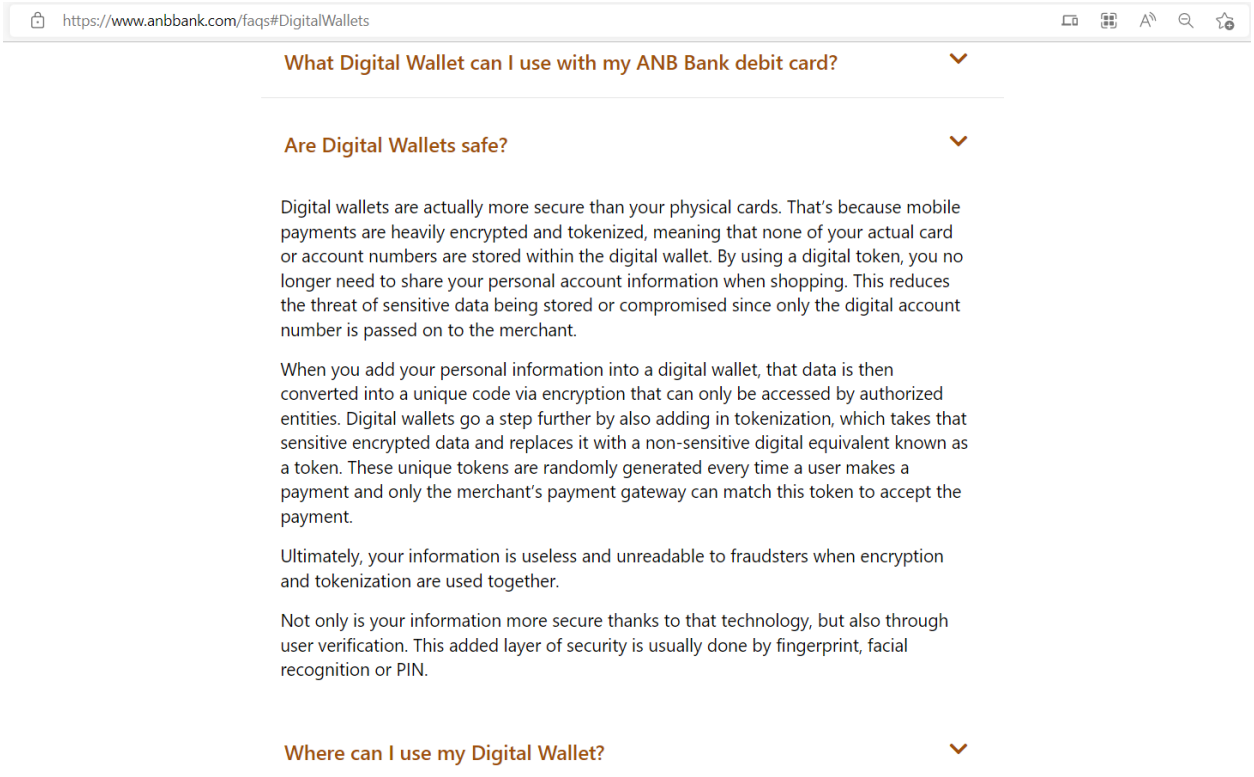
(Source: https://www.anb.com/Mobile-Pay.aspx)



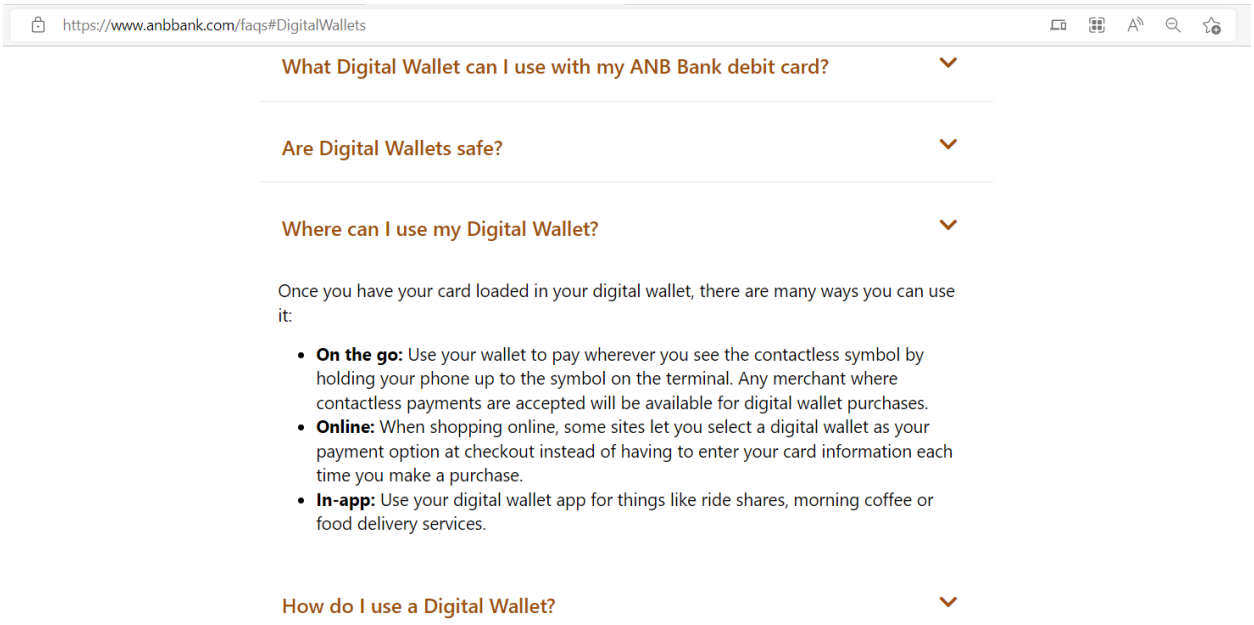
(Source: https://www.anbbank.com/online-and-mobile-banking/digital-wallets/apple-pay)



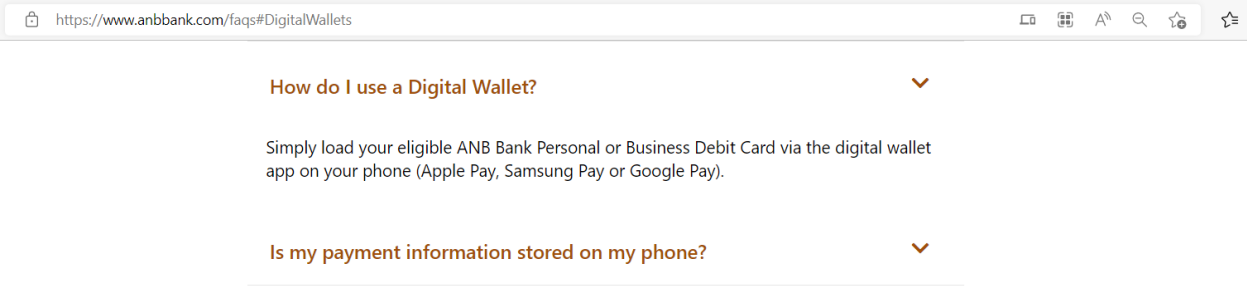
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)



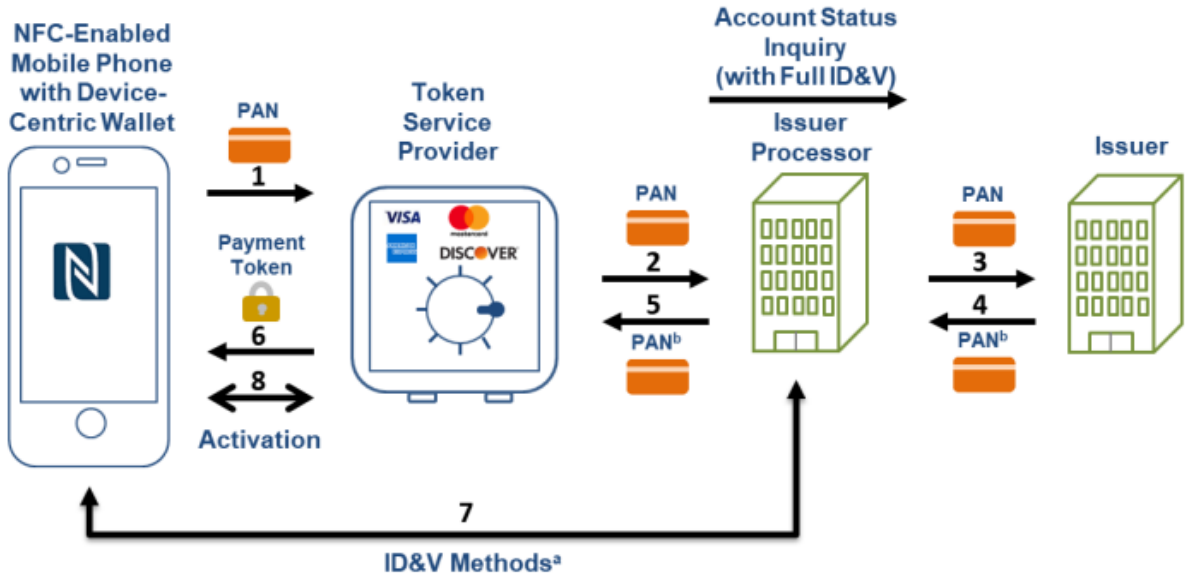
(Source: https://www.anbbank.com/faqs#DigitalWallets)



(Source: https://www.anbbank.com/faqs#DigitalWallets)

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

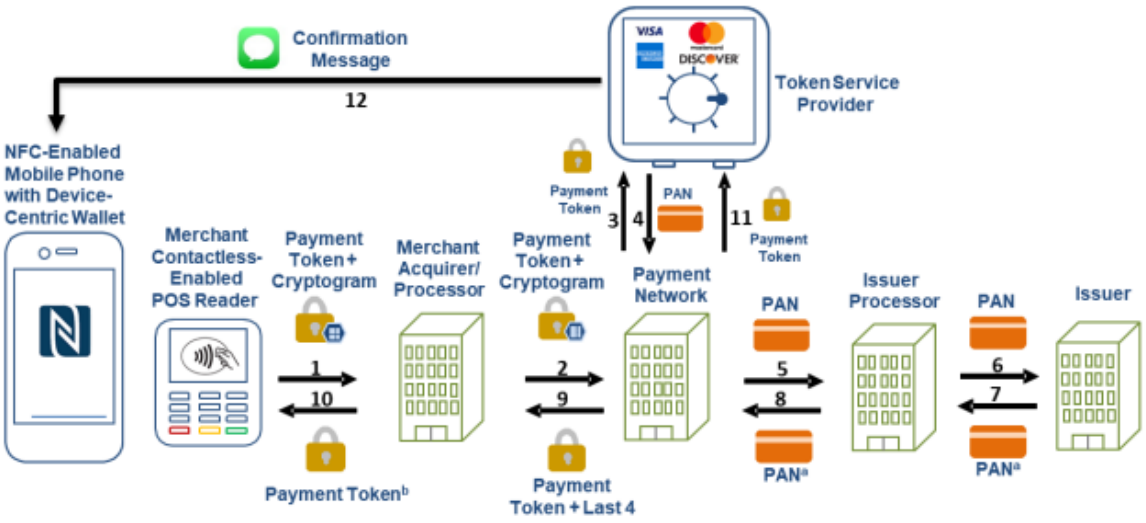
   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.



[a] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response
[b] Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

(Source: https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf)

95. The Accused Instrumentality includes a computer-implemented system for a user to authorize a service client's access to a secured resource associated with a common identifier without transmitting or otherwise providing the secured resource's common identifier to the service client. For example, a ANB account holder requests ANB to provision a specific ANB debit and/or credit card for use on his or her mobile device. The account holder can then request for payment to be made by ANB to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder using his or her smartphone

when near the NFC merchant terminal at a checkout counter. In initiating the request, the account holder's smartphone receives certain transaction specific information from the merchant terminal, which is incorporated into a cryptogram generated by the smartphone that it transmits to the merchant's terminal, along with the token value, for forwarding to a messaging gateway. The merchant also inputs into the request the token value that was transmitted from the user's smartphone to the merchant's terminal using NFC. Thus, the request messages will include both the transaction specific cryptogram as well as token and transaction specific information sent that was used in making the cryptogram. At no time is the debit and/or credit card account number transmitted or otherwise provided to the merchant.

96. The Accused Instrumentality includes at least one interface adapted to receive and transmit data in communication with a user's application, a service client's application, or both. For example, the Accused Instrumentality includes an interface that is programmed to receive and transmit data in communication with a ANB card account holder's mobile device, a merchant's payment terminal software and/or hardware, or both. The interface is also programmed to receive requests initiated by ANB card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder. This interface is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

97. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one secured resource identifier associated with the

common identifier of the secured resource, wherein the common identifier and secured resource identifier are not the same. For example, the Accused Instrumentality includes a server that is programmed to receive registration information, including the name on the debit and/or credit card, the debit and/or credit card account number (which has a corresponding token), and the CVV number received from ANB card account holders through the interface for provisioning a specific ANB debit and/or credit card for use on their mobile devices. The server is also programmed to receive requests initiated by ANB card account holders for payment to be made to a specific merchant in a specific amount for a specific transaction from a specific ANB card account of the account holder. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

98. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the secured resource by the service client, the authorization request message having been received through the at least one interface from the user's application and comprising: a first service client identifier; a first transaction specific information; the user identifier; and a designated secured resource identifier selected from one of the at least one secured resource identifiers. For example, the Accused Instrumentality includes a server that is programmed to receive an authorization request message having been received through the at least one interface and originating from the ANB card account holder's mobile device. The server is programmed to receive authorization requests initiated by ANB card account holders for payment to be made to a specific merchant, the request including at least one piece of specific transaction information for a specific transaction,

a token, a CVV number, a merchant identifier, other token information, and the ANB card account holder identifier. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

99. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to generate a first transaction specific authentication credential associated with the authorization request, whereby the first transaction specific authentication credential comprises a key string and does not include or reveal the common identifier associated with the designated secured resource identifier. For example, the Accused Instrumentality includes a server that is programmed to identify within the payment authorization request the transaction specific information that was passed by the merchant, and the server will generate a cryptogram using at least some of that transaction specific information. The cryptogram is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the token. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

100. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to receive an access request message from the service client's application through the at least one interface, the payment request message comprising: a second service client identifier; a second transaction specific information; and a second transaction specific authentication credential whereby the second transaction specific authentication credential was received by the service client's

application from the user's application. For example, the Accused Instrumentality includes a server that is programmed to receive a payment request message from the merchant's payment application through the at least one interface. The payment request message includes a merchant identifier, a second piece of transaction specific information from a specific transaction, and a cryptogram that was received by the merchant application from the ANB card account holder's mobile device. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to receive the messages.

101. The Accused Instrumentality includes one or more servers in secure communication with the at least one interface, the one or more servers having a third instruction embodied in a computer readable medium, the third instruction operable to validate the user's request to access the secured resource associated with the designated secured resource identifier without transmitting or otherwise providing the common identifier of the secured resource to the service client by determining if: the first service client identifier matches the second service client identifier; the first transaction specific information matches the second transaction specific information; and the first transaction specific authentication credential matches the second transaction specific authentication credential. For example, the server attempts to match the payment request merchant identifier to the authorization request merchant identifier, the payment request transaction specific information to the authorization request transaction specific information, and the server generated cryptogram to the cryptogram sent with the payment request message. If there are matches for all three, the server authenticates the identity of requestor as the actual account holder. The server is either hosted directly by ANB or through an agent with whom ANB has contracted to provide the authentication services.

102. Moreover, Plaintiff alleges that each of these elements are present in the Accused Instrumentality either literally or under the doctrine of equivalents if anywhere determined not to be literally present. For example, if a function literally claimed to be performed by a given element, such as a particular server or set of instructions, is conducted in the accused system by another server or another set of instructions, Plaintiff alleges that this would be an infringement under the doctrine of equivalents because the two would be substantially the same and would be performing the same function in the same way to arrive at the same result.

103. Defendants thus infringe one or more claims of the 454 Patent. For example, the elements and conduct described herein are covered by and infringe upon at least Claim 8 of the 454 Patent. Thus, Defendant's use, manufacture, sale, and/or offer for sale of the Accused Instrumentality is enabled by the system described in the 454 Patent.

104. ANB has directly infringed and continues to directly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(a), by making, using, importing, offering for sale, and/or selling the Accused Instrumentality without authority in the United States and will continue to do so unless enjoined by this Court.

105. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) at least Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(b), by actively inducing the infringement of the 454 Patent by others and ANB will continue to do so unless enjoined by this Court. ANB's deliberate and/or willfully blind actions include, but are not limited to, actively marketing to, supplying, causing the supply to, encouraging, recruiting, and instructing others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers to use, make available for another's use, promote, market, distribute, import, sell and/or offer to sell the Accused

Instrumentality. These actions, individually and/or collectively, have induced and continue to induce the direct infringement of the 454 Patent by others such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers. ANB knew and/or was willfully blind to the fact that the induced parties' use, making available for another's use, promotion, marketing, distributing, importing, selling and/or offering to sell the Accused Instrumentality would infringe the 454 Patent.

106. ANB continues to make, use, make available for another's use, or sell or offer to sell, the Accused Instrumentality, and/or continues to induce others such as consumers, businesses, distributors, agents, sales representatives, account holders, end users and customers to infringe one or more claims of the 454 Patent.

107. ANB has indirectly infringed and continues to indirectly infringe (either literally or under the doctrine of equivalents) Claim 8 of the 454 Patent, in violation of 35 U.S.C. § 271(c), by contributing to the direct infringement of the 454 Patent by others, such as consumers, businesses, distributors, agents, sales representatives, end-users, account holders and customers, by offering to sell or selling within the United States the Accused Instrumentality which is a component of a patented machine, manufacture, combination, or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

108. ANB has committed these acts of infringement without license or authorization.

109. By engaging in the conduct described herein, ANB has caused injury to Textile and Textile has been damaged and continues to be damaged as result thereof and ANB is thus liable to Textile for infringement of the 454 Patent, pursuant to 35 U.S.C. § 271.

110. As a direct and proximate result of ANB's infringement of the 454 Patent, Textile has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate Textile for ANB's past infringement pursuant to 35 U.S.C. § 284, but in no event less than a reasonable royalty, together with interest and costs.

111. In addition, the infringing acts and practices of ANB have caused, are causing, and, unless such acts or practices are enjoined by the Court, will continue to cause immediate and irreparable harm and damage to Textile for which there is no adequate remedy at law, and for which ANB is entitled to injunctive relief pursuant to 35 U.S.C. § 283. As such, Textile is entitled to compensation for any continuing and/or future infringement up until the date that ANB is finally and permanently enjoined from further infringement.

112. ANB has had actual knowledge of the 454 Patent at least as of the date when it was notified of the filing of this action. By the time of trial, ANB will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the 454 Patent.

113. ANB has also indirectly and willfully infringed, and continues to indirectly and willfully infringe, the 454 Patent, as explained further below in the "Additional Allegations Regarding Infringement" section.

114. Textile has been damaged as a result of the infringing conduct by ANB alleged above. Thus, ANB is liable to Textile in an amount that adequately compensates it for such

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

115. Textile is entitled to collect pre-filing damages for the full period allowed by law for infringement of the 454 Patent.

ADDITIONAL ALLEGATIONS REGARDING INFRINGEMENT

116. ANB has also indirectly infringed the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by inducing others to directly infringe the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. ANB has induced the end-users, ANB's customers, to directly infringe (literally and/or under the doctrine of equivalents) the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by using the Accused Instrumentality.

117. ANB took active steps, directly and/or through contractual relationships with others, with the specific intent to cause them to use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

118. Such steps by ANB included, among other things, advising or directing customers and end-users to use the Accused Instrumentality in an infringing manner; advertising and promoting the use of the Accused Instrumentality in an infringing manner; and/or distributing instructions that guide users to use the Accused Instrumentality in an infringing manner.

119. ANB has performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts constitute infringement, at least since the filing of the Complaint.

120. ANB was and is aware that the normal and customary use of the Accused Instrumentality by ANB's customers would infringe the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. ANB's inducement is ongoing.

121. ANB directs or controls the use of the Accused Instrumentality nationwide through its own websites and in its own branches, including in Texas and elsewhere in the United States, and expects and intends that the Accused Instrumentality will be so used.

122. ANB took active steps, directly and/or through contractual relationships with others, with the specific intent to cause such persons to make or use the Accused Instrumentality in a manner that infringes one or more claims of the patents-in-suit, including, for example, at least Claim 1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

123. ANB performed these steps, which constitute induced infringement, with the knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and with the knowledge that the induced acts would constitute infringement.

124. ANB's inducement is ongoing.

125. ANB has also indirectly infringed by contributing to the infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent. ANB has contributed to the direct infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by the end-user of the Accused Instrumentality.

126. The Accused Instrumentality has special features that are specially designed to be used in an infringing way and that have no substantial uses other than ones that infringe the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent, including, for example, at least Claim

1 of the 079 Patent, Claim 1 of the 802 Patent, Claim 9 of the 659 Patent, and Claim 8 of the 454 Patent.

127. As described above, the special features include securely authorizing specific transactions without providing a credit or debit card number to the merchant used in a manner that infringes the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent.

128. The special features constitute a material part of the invention of one or more of the claims of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

129. ANB's contributory infringement is ongoing.

130. ANB has had knowledge of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent at least since the filing of the Complaint.

131. ANB's customers have infringed the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent.

132. ANB encouraged its customers' infringement.

133. ANB's direct and indirect infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent is, has been, and/or continues to be willful, intentional, deliberate, and/or in conscious disregard of Textile' rights under the patents.

134. Textile has been damaged as a result of the infringing conduct by ANB alleged above. Thus, ANB is liable to Textile in an amount that adequately compensates it for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Textile hereby requests a trial by jury on all issues so triable by right.

PRAYER FOR RELIEF

Textile requests that the Court find in its favor and against ANB, and that the Court grant Textile the following relief:

a. Judgment that one or more claims of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent have been infringed, either literally and/or under the doctrine of equivalents, by ANB and/or all others acting in concert therewith;

b. A permanent injunction enjoining ANB and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert therewith from infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent; or, in the alternative, an award of a reasonable ongoing royalty for future infringement of the 079 Patent, the 802 Patent, the 659 Patent, and the 454 Patent by such entities;

c. Judgment that ANB account for and pay to Textile all damages to and costs incurred by Textile because of ANB's infringing activities and other conduct complained of herein, including an award of all increased damages to which Textile is entitled under 35 U.S.C. § 284;

d. That Textile be granted pre-judgment and post-judgment interest on the damages caused by ANB's infringing activities and other conduct complained of herein;

e. That this Court declare this an exceptional case and award Textile its reasonable attorney's fees and costs in accordance with 35 U.S.C. § 285; and

f. That Textile be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: September 12, 2022 Respectfully submitted,

/s/ *Matthew J. Antonelli*
Matthew J. Antonelli
Texas Bar No. 24068432
matt@ahtlawfirm.com
Zachariah S. Harrington
Texas Bar No. 24057886
zac@ahtlawfirm.com
Larry D. Thompson, Jr.
Texas Bar No. 24051428
larry@ahtlawfirm.com
Christopher Ryan Pinckney
Texas Bar No. 24067819
ryan@ahtlawfirm.com
ANTONELLI, HARRINGTON
& THOMPSON LLP
4306 Yoakum Blvd., Ste. 450
Houston, TX 77006
(713) 581-3000

Stafford Davis
State Bar No. 24054605
sdavis@stafforddavisfirm.com
Catherine Bartles
Texas Bar No. 24104849
cbartles@stafforddavisfirm.com
THE STAFFORD DAVIS FIRM
815 South Broadway Avenue
Tyler, Texas 75701
(903) 593-7000
(903) 705-7369 fax

Attorneys for Textile Computer Systems, Inc.